UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF INTERPRETATION OF RELIABILITY STANDARD CIP-002-5.1a

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
charles.berardesco@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

November 28, 2016

TABLE OF CONTENTS

I. NOTICES AND COMMUNICATIONS 2
II. BACKGROUND 2
A. Regulatory Framework 2
B. Interpretation Procedural History 3
III. JUSTIFICATION FOR APPROVAL 4
A. EnergySec RFI of Criterion 2.1 of Attachment 1 to CIP-002-5.1 4
B. Proposed Interpretation 5
IV. CONCLUSION 7

Exhibit A Proposed Reliability Standard CIP-002-5.1a

Exhibit B Complete Record of Development

Exhibit C Interpretation Drafting Team Roster

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF INTERPRETATION OF RELIABILITY STANDARD CIP-002-5.1

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA")[1] and Section 39.5[2] of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"), the North American Electric Reliability Corporation ("NERC") hereby submits for Commission approval a proposed interpretation of Reliability Standard CIP-002-5.1.[3] The proposed interpretation provides clarification regarding the meaning of the phrase "shared BES Cyber Systems" in Criterion 2.1 of Attachment to Reliability Standard CIP-002-5.1.[4] As discussed further below, the proposed interpretation provides that: (1) the phrase "shared BES Cyber Systems" in Criterion 2.1 refers to discrete BES Cyber Systems that are shared by multiple generation units; and (2) the evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System.

NERC requests that the Commission approve the proposed interpretation appended to CIP-002-5.1a (**Exhibit A**) and find that the proposed interpretation is just, reasonable, not unduly

---

[1] 16 U.S.C. § 824o (2012).

[2] 18 C.F.R. § 39.5 (2016).

[3] The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

[4] Unless otherwise designated, capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("*NERC Glossary*"), *available at* http://www.nerc.com/files/Glossary_of_Terms.pdf.

discriminatory or preferential, and in the public interest. NERC requests that the proposed interpretation become effective upon Commission approval.[5]

As required by Section 39.5(a)[6] of the Commission's regulations, this petition presents the technical basis and purpose of the proposed interpretation and the complete record of development (**Exhibit B**). The proposed interpretation was adopted by the NERC Board of Trustees on November 2, 2016.

I. NOTICES AND COMMUNICATIONS

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

Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
shamai.elstein@nerc.net

II. BACKGROUND

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[7] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Bulk Power System, and with the duties of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1)[8] of the FPA states that all users, owners, and operators of the Bulk Power System in the United States will be

---

[5] Consistent with NERC numbering convention, upon approval of the proposed interpretation, the standard number would be CIP-002-5.1a.

[6] 18 C.F.R. § 39.5(a) (2016).

[7] 16 U.S.C. § 824o (2012).

[8] *Id.* § 824o(b)(1).

subject to Commission-approved Reliability Standards. Section 215(d)(5)[9] of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard. Section 39.5(a)[10] of the Commission's regulations requires the ERO to file with the Commission for its approval each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes should be made effective.

The Commission is vested with the regulatory responsibility to approve Reliability Standards that protect the reliability of the Bulk Power System and to ensure that Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA[11] and Section 39.5(c)[12] 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.

B. Interpretation Procedural History

The Commission approved Reliability Standard CIP-002-5.1 in Order No. 791, issued on November 22, 2013.[13] On March 3, 2015, as amended on May 8, 2015, Energy Sector Security Consortium, Inc. ("EnergySec") filed a Request for Interpretation ("RFI") of Reliability Standard CIP-002-5.1 seeking clarification regarding the use of the phrase "shared BES Cyber Systems" in Criterion 2.1 of Attachment 1 to the standard. The NERC Standards Committee accepted the RFI on September 23, 2015 and directed the existing standard drafting team working on revisions to

---

9 *Id.* § 824o(d)(5).

10 18 C.F.R. § 39.5(a) (2016).

11 16 U.S.C. § 824o(d)(2).

12 18 C.F.R. § 39.5(c)(1).

13 *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and rehearing*, Order No. 791-A, 146 FERC ¶ 61, 188 (2014).

the CIP Reliability Standards to act as the interpretation drafting team for purposes of the EnergySec RFI.

The proposed interpretation was posted for a 45-day comment period and ballot, ending on September 12, 2016. The proposed interpretation achieved a 75.43% quorum and 91.68% approval from stakeholders. Pursuant to the NERC Rules of Procedure, the proposed interpretation was posted for a 10-day final ballot from October 13, 2016 through October 24, 2016, resulting in a 81.25% quorum and 91.31% approval. The proposed interpretation was approved by the NERC Board of Trustees on November 2, 2016.

III. JUSTIFICATION FOR APPROVAL

The purpose of Reliability Standard CIP-002-5.1 is to identify and categorize BES Cyber Systems and their associated BES Cyber Assets 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 reliable operation of the Bulk Electric System. Attachment 1 to the standard sets forth the criteria used to categorize BES Cyber Systems into impact categories (i.e., high, medium or low impact). The proposed interpretation provides clarity regarding the application of Criterion 2.1 of Attachment 1. NERC respectfully requests that the Commission approve the proposed interpretation as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

A. EnergySec RFI of Criterion 2.1 of Attachment 1 to CIP-002-5.1

Criterion 2.1 of Attachment 1 provides that BES Cyber Systems associated with the following should be categorized as medium impact:

> Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes,

> adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

EnergySec's RFI posed the following questions with respect to the meaning of the phrase "shared BES Cyber Systems" in the second sentence of Criterion 2.1:

1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

B. Proposed Interpretation

In response to the EnergySec RFI, Reliability Standard CIP-002-5.1a adds an interpretation as Appendix 1 to the standard that clarifies that: (1) the phrase "shared BES Cyber Systems" in Criterion 2.1 refers to discrete BES Cyber Systems that are shared by multiple generation units; and (2) the evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. The proposed interpretation thus incorporates, into the standard document, the explanation that an entity must separately evaluate each BES Cyber System under Criterion 2.1 to determine whether the BES Cyber System is shared by – i.e., used by or could affect – more than one unit at a generating plant.

Specifically, in response to the first question posed by EnergySec, the proposed interpretation provides as follows:

> The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:

> 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.

In response to the second question, the proposed interpretation clarifies that "[t]he phrase 'shared BES Cyber Systems' refers to discrete BES Cyber Systems that are shared by multiple generation units." The proposed interpretation also notes that NERC's Frequently Asked Questions document issued to support implementation of the CIP Reliability Standards approved in Order No. 791 (the "CIP FAQs") also address the meaning of the phrase "shared BES Cyber System."[14] Specifically, the proposed interpretation cites FAQ #49, which provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR." Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: Impact Rating of Generation Resource Shared BES Cyber Systems for further information and examples.[15]

In short, the interpretation clarifies that a "shared BES Cyber System" under Criterion 2.1 is a BES Cyber System that, if rendered unavailable, degraded, or misused, could affect the operation of

---

[14] The CIP FAQs are available at http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPV5_FAQs_Consolidated_Oct2015_Oct_13_2015.pdf.

[15] CIP FAQs at 2.

more than one unit at a generation plant. As explained in the NERC Lesson Learned document referenced in FAQ #49, "[i]dentifying shared BES Cyber Systems involves detailed analysis that considers shared generating plant operational processes (e.g., air, water, steam, environmental, and fuel handling processes) and electronic connectivity."

As the proposed interpretation clarifies that the phrase "shared BES Cyber Systems" applies to each discrete BES Cyber System, not collectively to groups of BES Cyber Systems, the third question in the RFI is moot.

IV. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission approve the proposed interpretation appended to regional Reliability Standard CIP-002-5.1a (Exhibit A hereto), effective upon Commission approval. The proposed interpretation provides additional clarity and would facilitate consistent application of Criterion 2.1.

Respectfully submitted,

/s/ Shamai Elstein

Charles A. Berardesco
Senior Vice President and General Counsel
Shamai Elstein
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
charles.berardesco@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

November 28, 2016

Exhibit A

Proposed Reliability Standard CIP-002-5.1a

CIP-002-5.1a

Clean and Redline Versions

CIP-002-5.1a

Clean Version

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5.1a

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets 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 reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in 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 functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5.1a:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3. 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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

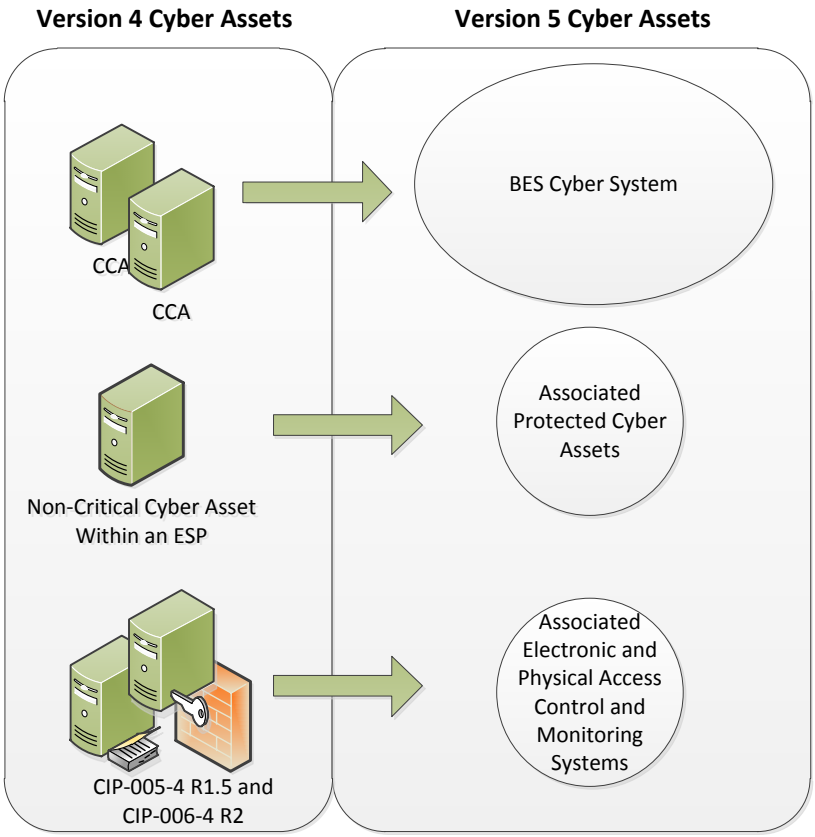
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it 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.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly	Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5.1a - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

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

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

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. 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 or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, 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.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service 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. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service 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 Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service 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 (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service 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:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

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) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control 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
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service 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:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure 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:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure 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:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is 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 supports 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 consider 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 supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System 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.

<u>High Impact Rating (H)</u>

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. 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 as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

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 Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. 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.

  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, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation 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.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. 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 Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for 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.

- Criterion 2.4 includes BES Cyber Systems for 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 in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) 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 facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion 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 significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.

  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA

  - 345 kV –> 1,300 MVA

  - 500 kV –> 2,000 MVA

  - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

  - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate

connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for 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.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, 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.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for 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 BES Cyber Systems 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.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, 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 underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to 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. 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 medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  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. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

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. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.
- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. 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.

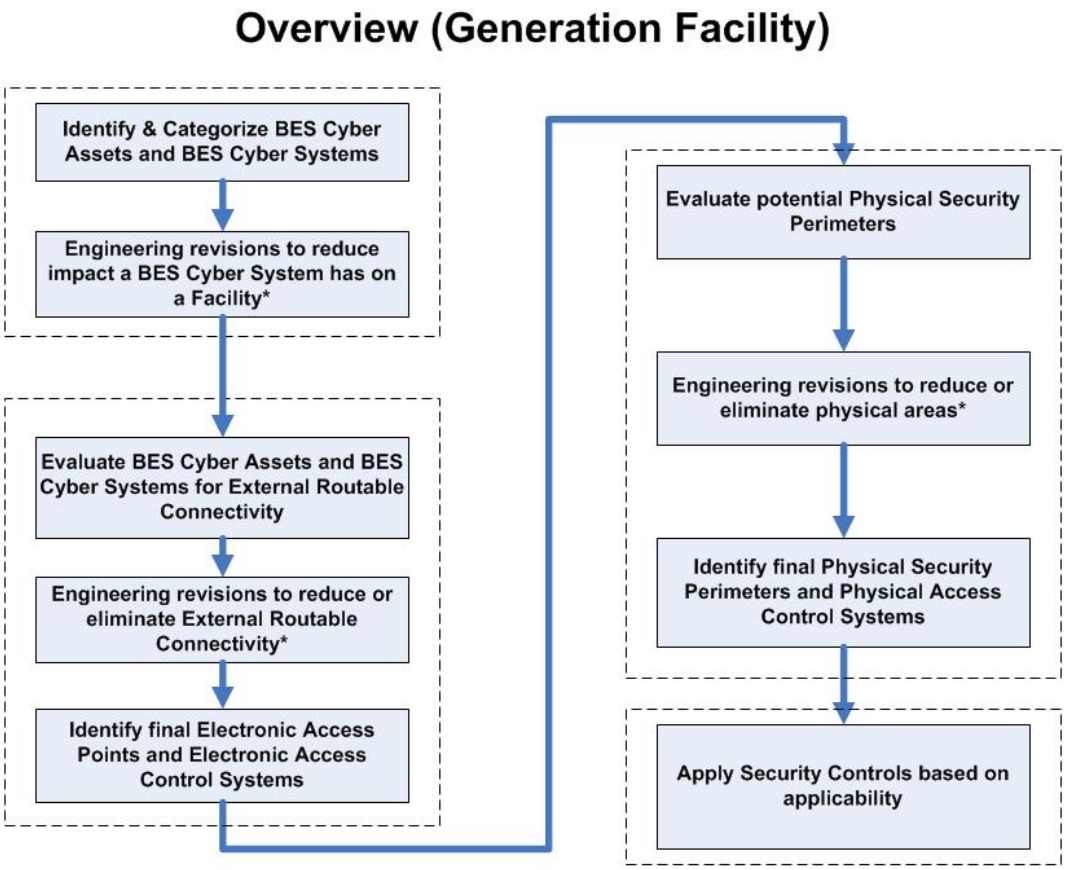
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements 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, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope 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.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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.	
3	12/16/09	Updated version number from -2 to -3.	Update

		Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
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.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	

Appendix 1

Requirement Number and Text of Requirement
<u>CIP-002-5.1, Requirement R1</u> R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required). <u>Attachment 1, Criterion 2.1</u> 2. Medium Impact Rating (M) Each BES Cyber System, not included in Section 1 above, associated with any of the following: 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions
Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems." The Interpretation Drafting Team identified the following questions in the RFI: 1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems? 2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units? 3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?
Responses
Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems? The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added) Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides: > 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.

Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

CIP-002-5.1a

Redline Version

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5.1a

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets 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 reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in 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 functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-5.1a:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3. 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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

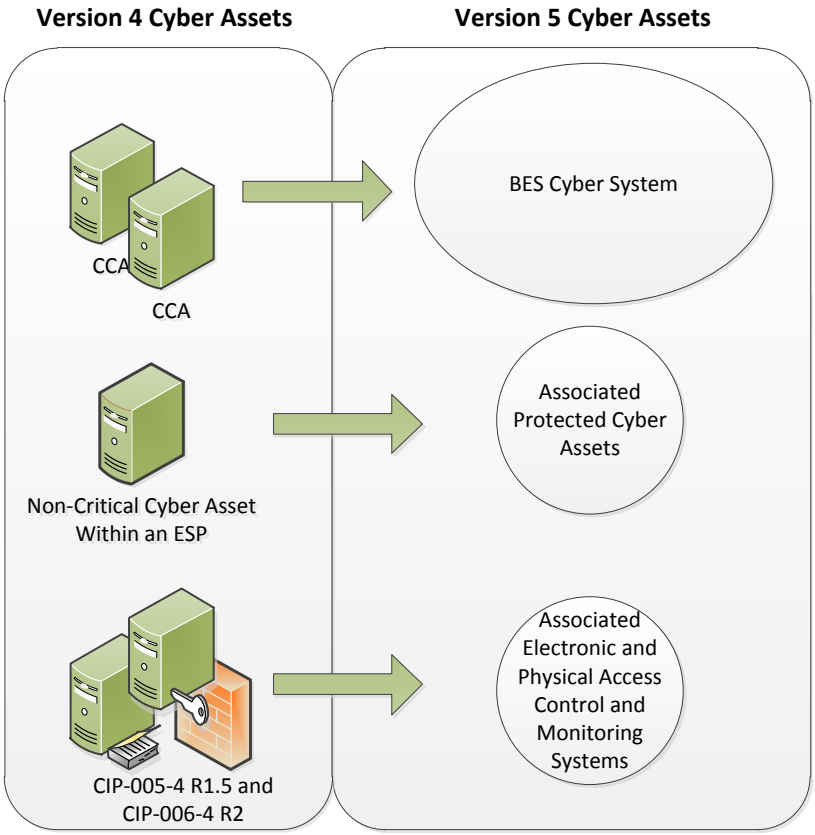
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it 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.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly	Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1a)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5.1a - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

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

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

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. 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 or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, 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.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service 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. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service 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 Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service 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 (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service 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:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

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) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control 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
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service 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:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure 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:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure 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:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is 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 supports 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 consider 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 supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System 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.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. 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 as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

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 Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. 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.

  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, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation 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.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. 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 Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for 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.

- Criterion 2.4 includes BES Cyber Systems for 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 in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) 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 facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion 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 significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.

  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA

  - 345 kV –> 1,300 MVA

  - 500 kV –> 2,000 MVA

  - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

  - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate

connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for 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.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, 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.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for 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 BES Cyber Systems 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.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, 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 underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to 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. 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 medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  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. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

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. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.
- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. 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.

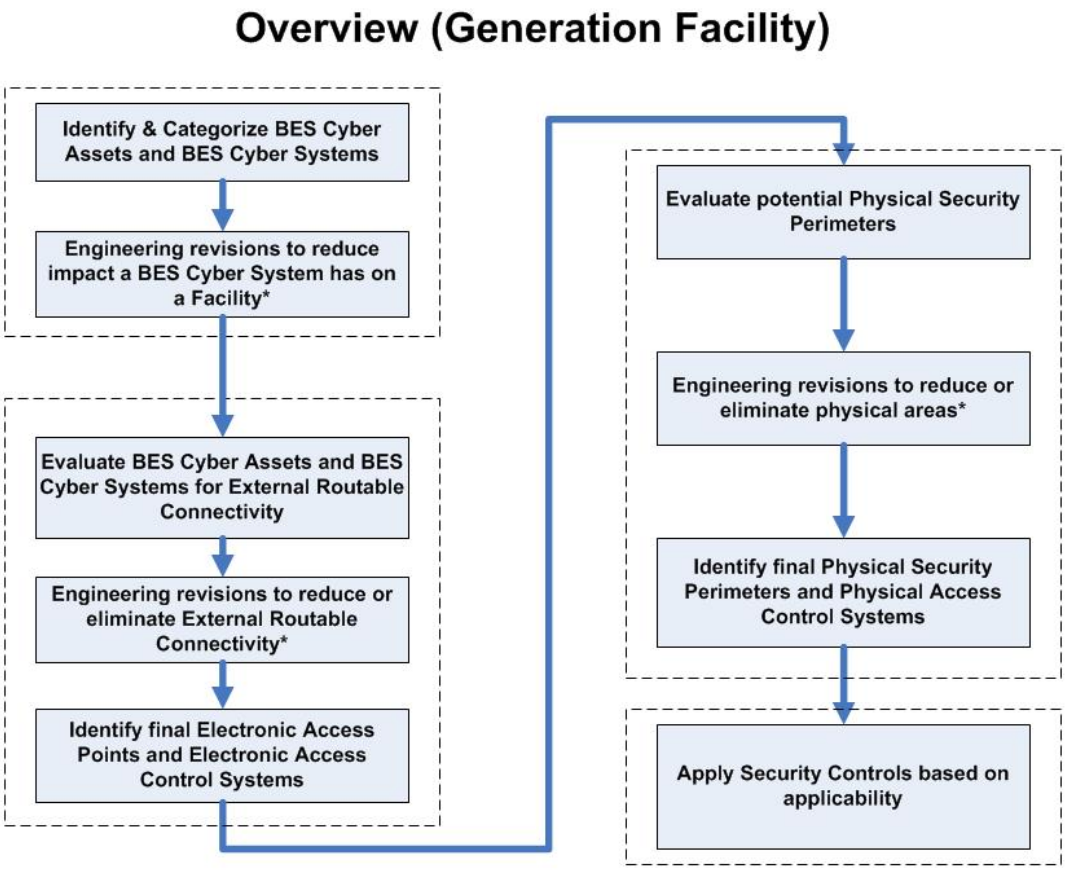
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements 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, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope 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.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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.	
3	12/16/09	Updated version number from -2 to -3.	Update

		Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
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.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced "Devices" with "Systems" in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	

Appendix 1

Requirement Number and Text of Requirement
CIP-002-5.1, Requirement R1 R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required). Attachment 1, Criterion 2.1 2. Medium Impact Rating (M) Each BES Cyber System, not included in Section 1 above, associated with any of the following: 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."

The Interpretation Drafting Team identified the following questions in the RFI:

1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?
2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?
3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Responses

Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:

> 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.

Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

Exhibit B

Complete Record of Development

Project 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)

Related Files

Status

The final ballot for the **Interpretation of CIP-002-5.1** concluded **8 p.m. Eastern, Monday, October 24, 2016**. The voting results can be accessed via the link below. The interpretation will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background

EnergySec submitted a Request for Interpretation (RFI) seeking clarity regarding CIP-002-5.1, Requirement 1, Attachment 1, Part 2.1. The Standards Committee accepted the RFI of CIP-002-5.1 at the September 23, 2015 meeting. Thereafter, the Project Management and Oversight Subcommittee (PMOS) assigned the RFI a medium- to low- priority project.

Standard Affected: CIP-002-5.1 - Cyber Security — BES Cyber System Categorization

Purpose / Industry Need

The RFI asks whether the language "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or whether instead it refers to groups of BES Cyber Systems that, collectively, could impact multiple units. Essentially, the RFI seeks clarity regarding whether the evaluation required under Requirement R1 should be performed individually for each discrete BES Cyber System at a single plant location, or instead, applied collectively for groups of BES Cyber Systems.

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft Interpretation**(10)**	Final Ballot Info**(11)** Vote	10/13/16 - 10/24/16	Ballot Results**(12)**	

Draft 1 Interpretation**(1)** Request for Interpretation**(2)** **Supporting Documents** Unofficial Comment Form (Word)**(3)** CIP-002-5.1**(4)**	Initial Ballot Info**(5)** Vote	09/02/16 – 09/12/16	Ballot Results**(7)**	Consideration of Comments**(9)**
	Comment Period Info**(6)** Submit Comments	07/27/16 – 09/12/16	Comments Received**(8)**	
	Join Ballot Pool	07/27/16 – 08/25/16		

Appendix 1

Interpretation of CIP-002-5.1, Requirement R1, Attachment 1, Criterion 2.1

Requirement Number and Text of Requirement
<u>CIP-002-5.1, Requirement R1</u> R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required). <u>Attachment 1, Criterion 2.1</u> 2. Medium Impact Rating (M) Each BES Cyber System, not included in Section 1 above, associated with any of the following: 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions
Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems." The Interpretation Drafting Team identified the following questions in the RFI: 1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems? 2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units? 3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?
Responses
Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems? The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added) Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides: > 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.

Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

When completed, email this form to: sarcomm@nerc.com

Note: an Interpretation cannot be used to change a standard.

Interpretation 2010-xx: Request for an Interpretation of [Insert Standard Number], Requirement Rx, for [Insert Name of Company]
Date submitted: March 3, 2015 (amended May 8, 2015)
Contact information for person requesting the interpretation:
Name: Steven Parker
Organization: Energy Sector Security Consortium, Inc (EnergySec)
Telephone: 503.621.8179
Email: steve@energysec.org
Identify the standard that needs clarification:
Standard Number (include version number): CIP-002-5.1 (example: PRC-001-1)
Standard Title: Cyber Security — BES Cyber System Categorization
Identify specifically what requirement needs clarification:
Requirement Number and Text of Requirement: R1 For brevity, only relevant parts of the Requirement and Attachment 1 (incorporated by reference) are quoted here. Requirement 1, subpart 1.2 states, "Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2 …" Attachment 1 is incorporated into the requirement by reference. Attachment 1, Section 2, Criterion 2.1 states, "Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." Clarification needed: With respect to the exclusion clause of Criterion 2.1 limiting applicability, should the evaluation be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems? Stated differently, does the phrase "shared BES Cyber Systems" refer to discrete BES Cyber

Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Discussion

Criterion 2.1 introduces the concept of "shared BES Cyber Systems", but it is not clear what is meant by "shared". Additionally, Criterion 2.1 refers to such shared systems in the plural, making it unclear whether the intent was to apply the Criterion to groups of BES Cyber Systems, or simply to indicate that a single generating plant location could have multiple BES Cyber Systems that meet the Criterion.

Further adding to the uncertainty with this requirement are statements made within a NERC Lessons Learned document, "Impact Rating of Generation Resources", dated September 2, 2014. For example, the Lessons Learned document states:

> "If, for instance, the generation units and BES Cyber Systems are connected in a manner that could result in the loss of 1500 MW or more if **one or more** BES Cyber Systems at the plant were compromised or misused, then those shared BES Cyber Systems at the plant (i.e., those that can, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW) must be categorized as medium impact BES Cyber systems." (emphasis added)

In particular, the use of the phrase "one or more" suggests that a collective evaluation is required.

The aforementioned Lessons Learned document also states:

> "If a Responsible Entity adopts the segmentation approach, consistent with criterion 2.1, entities must provide evidence that BES Cyber Systems associated with any group of generating units at generating plants greater than 1500 MW are segmented effectively such that there are no **common mode vulnerabilities** that could result in the loss of 1500 MW or more of generation at a single plant." (emphasis added)

The reference to "common mode vulnerabilities" suggests that BES Cyber Systems should be evaluated as a group in some circumstances, but is unclear as "common mode vulnerabilities" is not a defined term.

The Lessons Learned document also states:

> "For example, Responsible Entities should consider physical locations that could present a single point of failure (e.g., common control rooms for multiple generating units) to determine what physical protections are appropriate."

Again, this language suggests that BES Cyber Systems may need to be evaluated in groups, for example, when multiple BES Cyber Systems are physically co-located.

The Lessons Learned document also contains a flow chart outlining a suggested process for evaluating BES Cyber Systems for impact ratings. That flow chart does not contain a process for grouping BES Cyber Systems for a collective evaluation, therefore suggesting that the impact assessment occurs individually for each discrete BES Cyber System.

A final Lessons Learned document was posted on January 29, 2015. Some of the language referred to above was removed in the final version, but the questions still remain. The final Lessons Learned document maintains the reference to the Guidelines section of the standard that refers to "BES Cyber Systems with common mode vulnerabilities". This

suggests that common mode vulnerabilities are evaluated in the context of groups of BES Cyber Systems.

In addition, the final Lessons Learned provides only two options, protecting all BES Cyber Systems at the medium level, or segmenting the units. The suggested evidence includes references to network segmentation and firewall rules. This suggests that for collections of BES Cyber Systems on a common network, the collective impact would be evaluated rather than their individual impact. Network isolation would be required to avoid this collective analysis.

On the other hand, FAQ 49, released for comment on April 1, 2015, states that a shared BES Cyber System is one that "affects two or more BES Facilities, such as multiple generation units." Likewise, FAQ 50 refers to common mode vulnerabilities as "Any systems that can affect two or more BES Facilities, such as multiple generation units. … Protection systems, fuel-handling systems, cooling water, and air systems are also examples that should be evaluated as common mode vulnerabilities." These responses support an assertion that BES Cyber Systems need only be evaluated individually.

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

The evaluation of BES Cyber Systems and assignment of impact ratings is a foundational requirement in version 5 of the CIP standards. A clear understanding of the Criteria, and their proper application is essential to ensure BES Cyber Systems are correctly rated so that the appropriate controls can be applied. Furthermore, in this case, confusion regarding a potential collective assessment, and the criteria and process for such an assessment, can lead not only to under or over rating of systems, but also significant expense in re-engineering plant systems and/or security controls.

A proper understanding of this Criterion is critical to ensure entities can comply with CIP-002-5 R1 without undue risk or expense.

Version History

Version	Date	Owner	Change Tracking
1	April 22, 2011		
1	May 27, 2014	Standards Information Staff	Updated template and email address for submittal.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)

Do not use this form for submitting comments. Use the electronic form to submit comments on the Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec) developed by the standards drafting team (SDT) for Project 2016-02 Modifications to CIP Standards. The electronic form must be submitted by **8 p.m. Eastern, Monday, September 12, 2016**.

Additional information is available on the project page. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675 here.

Background Information

EnergySec submitted a Request for Interpretation (RFI) seeking clarity regarding CIP-002-5.1, Requirement 1, Attachment 1, Part 2.1. The RFI asks whether the language "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or whether instead it refers to groups of BES Cyber Systems that, collectively, could impact multiple units. Essentially, the RFI seeks clarity regarding whether the evaluation required under Requirement R1 should be performed individually for each discrete BES Cyber System at a single plant location, or instead, applied collectively for groups of BES Cyber Systems.

The Standards Committee (SC) accepted the RFI at the September 23, 2015 meeting. However, on December 9, 2015, the SC endorsed deferring consideration of the RFI until the SDT for Project 2016-02 Modifications to CIP Standards was formed and could serve as the Interpretation Drafting Team (IDT).

In reviewing the RFI, the IDT identified three distinct questions within the request and developed this interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams.

The three questions are:

1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?
2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?
3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The IDT requests you review the RFI, the associated standard, and the proposed interpretation before answering the following questions. You do not have to answer all of the questions. Enter all comments in simple text format.

This posting is soliciting comments through a 45-day formal comment period with an initial ballot during the last 10 days of the comment period.

Questions

1. Do you agree with the response to **Question 1**? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No
   Comments:

2. Do you agree with the response to **Question 2**? If not please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No
   Comments:

3. Do you agree with the response to **Question 3**? If not please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No
   Comments:

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5.1

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets 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 reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in 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 functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-5.1:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3. 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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-002-5.1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5.1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

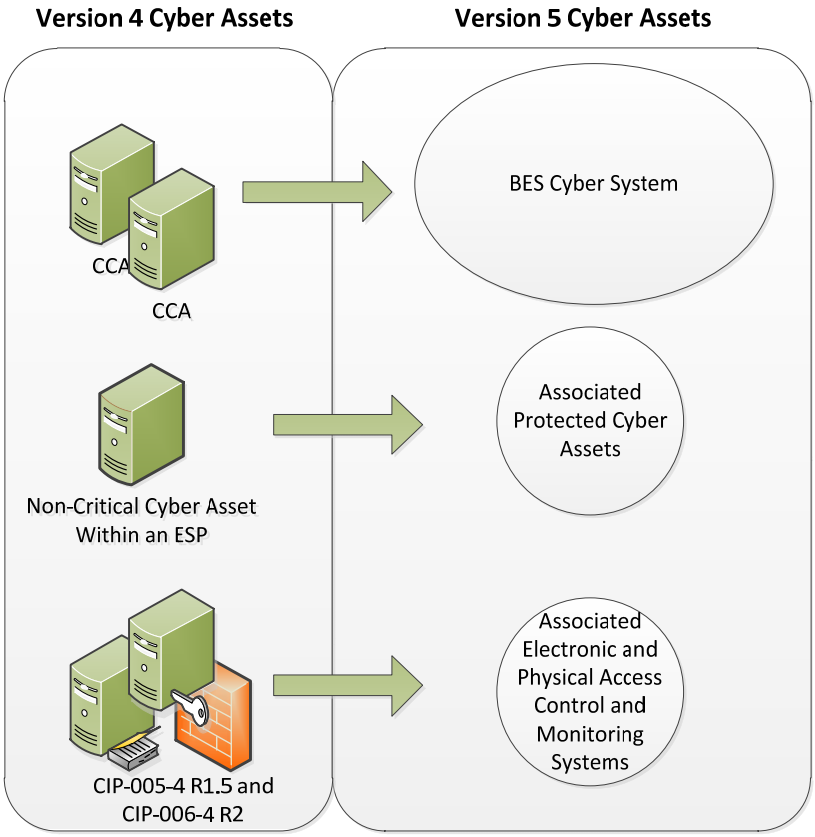
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it 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.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower	Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower	Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5.1 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

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

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

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. 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 or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, 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.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1

CIP-002-5.1 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5.1. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service 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. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service 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 Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service 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 (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service 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:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

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) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control 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
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service 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:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure 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:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure 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:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is 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 supports 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 consider 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 supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System 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.

<u>High Impact Rating (H)</u>

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. 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 as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

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 Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. 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.

  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, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation 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.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. 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 Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for 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.

- Criterion 2.4 includes BES Cyber Systems for 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 in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) 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 facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion 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 significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.

  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA

  - 345 kV –> 1,300 MVA

  - 500 kV –> 2,000 MVA

  - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

  - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities

would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for 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.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, 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.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for 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 BES Cyber Systems 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.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, 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 underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to 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. 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 medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  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. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

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. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to

restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. 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.

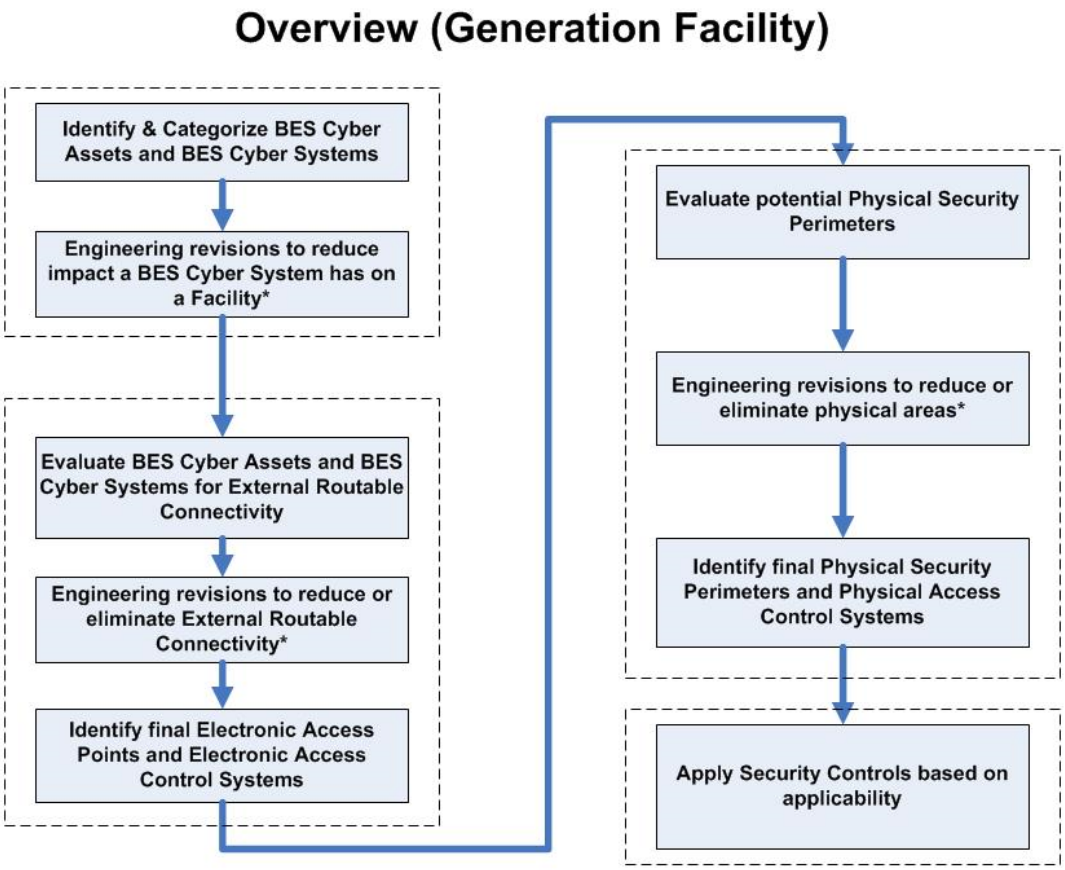
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements 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, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope 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.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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.	
3	12/16/09	Updated version number from -2 to -3.	Update

		Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
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.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1. (Order becomes effective on 2/3/14.)	

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-002-5.1 — Cyber Security — BES Cyber System Categorization

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-002-5.1	All	07/01/2016	

Printed On: November 21, 2016, 10:17 AM

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)

Formal Comment Period Open through September 12, 2016
Ballot Pools Forming through August 25, 2016

Now Available

A 45-day formal comment period for **Interpretation of CIP-002-5.1, is open through 8 p.m. Eastern, Monday, September 12, 2016.**

Commenting

Use the electronic form to submit comments on the interpretation. If you experience any difficulties using the electronic form, contact Nasheema Santos. An unofficial Word version of the comment form is posted on the project page.

Join the Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Thursday, August 25, 2016.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

An initial ballot for the interpretation will be conducted **September 2-12, 2016**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Al McMeekin or Stephen Crutchfield via (email).

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)

Formal Comment Period Open through September 12, 2016
Ballot Pools Forming through August 25, 2016

Now Available

A 45-day formal comment period for **Interpretation of CIP-002-5.1, is open through 8 p.m. Eastern, Monday, September 12, 2016.**

Commenting

Use the electronic form to submit comments on the interpretation. If you experience any difficulties using the electronic form, contact Nasheema Santos. An unofficial Word version of the comment form is posted on the project page.

Join the Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Thursday, August 25, 2016.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

An initial ballot for the interpretation will be conducted **September 2-12, 2016**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Al McMeekin or Stephen Crutchfield via (email).

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Survey: View Survey Results (/SurveyResults/Index/63)
Ballot Name: 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec) CIP-002-5.1 IN 1 INT
Voting Start Date: 9/2/2016 12:01:00 AM
Voting End Date: 9/12/2016 8:00:00 PM
Ballot Type: INT
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 218
Total Ballot Pool: 289
Quorum: 75.43
Weighted Segment Value: 91.68

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	70	1	38	0.95	2	0.05	0	10	20
Segment: 2	8	0.2	2	0.2	0	0	0	4	2
Segment: 3	62	1	33	0.892	4	0.108	2	11	12
Segment: 4	19	1	11	0.917	1	0.083	0	4	3
Segment: 5	70	1	31	0.886	4	0.114	3	11	21

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 6	46	1	22	0.815	5	0.185	0	6	13
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	1	0.1	0	0	0	1	0
Segment: 10	9	0.9	9	0.9	0	0	0	0	0
Totals:	289	6.5	150	5.959	16	0.541	5	47	71

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		Affirmative	N/A
1	Bonneville Power Administration	Donald Watkins		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		None	N/A
1	CMS Energy - Consumers Energy Company	Bruce Bugbee		Affirmative	N/A
1	Colorado Springs Utilities	Shawna Speer		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		None	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	None	N/A
1	JEA	Ted Hobson	Joe McClung	None	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Abstain	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAC Power	David Weekley	Scott Miller	Abstain	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		None	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		None	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Long Duong		Abstain	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Abstain	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Jennifer Wright	Harold Sherrill	Abstain	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		None	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Abstain	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Abstain	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Westar Energy	Kevin Giles		None	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	BC Hydro and Power Authority	Venkataramakrishnan Vinnakota		Abstain	N/A
2	California ISO	Richard Vine		None	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Michael DeLoach		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Julie Ross		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A

© 2016 - NERC Ver 3.0.1.6.Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Black Hills Corporation	Eric Egge		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		None	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Abstain	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Abstain	N/A
3	Gainesville Regional Utilities	Ken Simmons		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	Comments Submitted

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		None	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Ocala Utility Services	Randy Hahn		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Abstain	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Negative	Comments Submitted
3	Platte River Power Authority	Jeff Landis		None	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PNM Resources	Michael Mertz		None	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		Negative	No Comment Submitted
3	Puget Sound Energy, Inc.	Andrea Basinski		Abstain	N/A
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Negative	No Comment Submitted
3	Snohomish County PUD No. 1	Mark Oens		Abstain	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		None	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Abstain	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		None	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Austin Energy	Tina Garvey		Negative	Comments Submitted
4	CMS Energy - Consumers Energy Company	Julie Hegedus		Affirmative	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Abstain	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Abstain	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		None	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Abstain	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Matthew Finn		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	Black Hills Corporation	George Tatar		Negative	No Comment Submitted
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Bonneville Power Administration	Francis Halpin		None	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Negative	No Comment Submitted
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Abstain	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough		Abstain	N/A
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	No Comment Submitted
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Abstain	N/A
5	Muscatine Power and Water	Mike Avesing		Abstain	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Wayne Sipperly		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Leo Staples		Negative	Third-Party Comments
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Abstain	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer		Abstain	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Abstain	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		None	N/A
5	U.S. Bureau of Reclamation	Erika Doot		Abstain	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		None	N/A
5	Xcel Energy, Inc.	David Lemmons		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Negative	Comments Submitted

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Paul Huettl		None	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers		None	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Entergy	Julie Hall		None	N/A
6	Exelon	Maggy Powell		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Abstain	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Abstain	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		None	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		None	N/A
6	Platte River Power Authority	Sabrina Martz		None	N/A
6	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		None	N/A
6	Salt River Project	William Abraham		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		None	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Abstain	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Abstain	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 289 of 289 entries

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB02

Comment Report

Project Name:	2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)
Comment Period Start Date:	7/27/2016
Comment Period End Date:	9/12/2016
Associated Ballots:	2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec) CIP-002-5.1 IN 1 INT

There were 18 sets of responses, including comments from approximately 18 different people from approximately 18 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the response to Question 1? If not, please provide the basis for your disagreement and an alternate proposal.

2. Do you agree with the response to Question 2? If not please provide the basis for your disagreement and an alternate proposal.

3. Do you agree with the response to Question 3? If not please provide the basis for your disagreement and an alternate proposal.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC

					Brian Shanahan	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Sean Bodkin	Dominion	4	NPCC
ACES Power Marketing	Warren Cross	1,3,5,6	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Brazos Electric Power Cooperative, Inc.	BREC	1,5	Texas RE
					Prairie Power, Inc.	PPI	1,3	SERC
					Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					East Kentucky Power Cooperative	EKPC	1,3	SERC
					Sunflower Electric Power Corporation	SEPC	1	SPP RE
					Great River Energy	GRE	1,3,5,6	MRO

1. Do you agree with the response to Question 1? If not, please provide the basis for your disagreement and an alternate proposal.

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

As Austin Energy (AE) understands the question, EnergySec is asking whether the entity must determine:

1. Whether each discrete BES Cyber System "could, within 15 minutes, adversely impact the reliable operation" of generation units aggregating to ≥ 1500 MW; ***or***

2. Whether, collectively, groups of BES Cyber Systems at the generation facility "could, within 15 minutes, adversely impact the reliable operation" of generation units aggregating to ≥ 1500 MW.

The proposed response merely regurgitates the contents of the Background discussion regarding an entity's freedom to group BES Cyber Assets into BES Cyber Systems, it does not answer the question of how to determine if BES Cyber Systems are ***shared***.

AE *believes* the drafting team intended to say:

CIP-002-5.1 contains no *requirement* to *group* BES Cyber Systems. Accordingly, Responsible Entities may determine whether to consider BES Cyber Systems "shared." Consequently, a Compliance Enforcement Authority has no basis for questioning a Responsible Entity's conclusions regarding whether BES Cyber Systems are "shared" with respect to their ability to adversely impact the reliable operation of generation units aggregating to ≥ 1500 MW in a single Interconnection.

If AE has interpreted the proposed response correctly, the drafting team should clearly say so. If AE is not correct, the drafting team should rewrite the response to make it clearer.

Likes 0	
Dislikes 0	

Response

Diana McMahon - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP does not agree that the answer provided addresses the question. The question is not if an evaluation is to be done to determine if a BES Cyber system is shared. SRP understands the question to be asking whether the criterion should be performed on a discrete BES Cyber System shared by multiple generating units at a single plant location or on a collection of BES Cyber Systems shared by multiple generating units at a single plant location.

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3

Answer	No
Document Name	

Comment

Logical grouping of assets should be at the discretion of the entity and not a requirement

However, this ambiguity may not be supported at audit

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	No
Document Name	

Comment

We disagree that evaluation of each BES Cyber System needs to be performed individually for each discrete BES Cyber System. The question may be addressed by simply looking at the elements that comprise Criterion 2.1.

The Elements of Criterion 2.1 are:

Generation

- Commissioned generation
- A group [which we interpret as 1 or more] generating units
- The generating units are at a single plant location
- The generating units aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceed 1500 MW
- The 1500MW threshold is at a single Interconnection.

Relationship Between the Generation and the BES Cyber Systems

- The generating units share a BES Cyber System

The BES Cyber System

- The BES Cyber System can cause an adverse impact to the reliable operation of any combination of the generating units
- The adverse impact is within 15 minutes
- The aggregate adverse impact equals or exceeds 1500 MW
- The 1500MW adverse impact occurs at a single Interconnection.

In consideration of the criteria, if a single element is false / untrue, the BES Cyber System does not meet the threshold of a Medium Impact Risk. While we think that is straight forward, there is some nuance associated with the evaluation of a BES Cyber System, which is likely the genesis of the question.

The evaluation of a BES Cyber System.

The question asked for clarification of the term BES Cyber Systems, wanting to know if it means each individual and discrete BES Cyber System at a single plant location or collectively for groups of BES Cyber Systems.

We think clarification is found in Criterion 2.1 elements. For example, if there is a group of BES Cyber Systems and evaluation of the individual components determine the Criterion 2.1 thresholds are not met. At that point, it would be easy to say they are not a Medium Impact Risk. However, Criterion 2.1 language, paraphrased, is BES Cyber Systems that *could* adversely impact reliable operation of the generation units.

We feel the “could” qualifier brings into scope the relationship between and reliance upon the individual components of the group of BES Cyber Systems.

In other words:

If there is a failure in the interaction between two of the multiple BES Cyber Systems.

AND

The failure between the BES Cyber Systems “…within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection,”

AND

All other elements of Criterion 2.1 are met.

THEN

The threshold is pierced and the Medium Impact Risk is assigned.

It is Not Necessary to Evaluate Each Individual BES Cyber System

Based on the example, it may not be necessary to evaluate each individual BES Cyber System if the Criterion 2.1 threshold is breached on the potential failure of the interaction between two BES Cyber Systems.

We recognize the Criterion is specific to BES Cyber Systems and not the interaction between systems, but the “could” qualifier brings those interactions into scope of the evaluation regardless whether the individual BES Cyber System, alone, can cause the requisite adversity to reliability.

Resolution is Found in the Standard Revision Process

We believe the path to clarifying the ambiguous and uncertain language requires revision of Criterion 2.1 and the underlying Standard. The material revisions required to resolve the issues cannot be gained through the interpretation process.

Jointly-Owned Units Not Considered in Standard

Of additional concern are scenarios of jointly owned units (JOU) with BES Cyber Systems that communicate between entities and also meet Criterion 2.1. While contracts will delineate owners' responsibilities, it is common with JOU a level of parallel systems that, individually, "could" pierce the adverse reliability threshold.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

1. Initial ballot for CIP-003-7 - Cyber Security – Security Management Controls

Vote: No

Comments: PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets.

Likes 0	
Dislikes 0	

Response

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SCE agrees that a BES Cyber System that is shared between multiple generators needs to be evaluated individually, as opposed to being collectively grouped. Furthermore, SCE agrees that there is no obligation to group BES Cyber Systems. Each entity is given the choice of granularity in grouping BES Cyber Assets into BES Cyber Systems, but is not required to group BES Cyber Systems.

Likes 0	

Dislikes 0	
Response	
Jaclyn Massey - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
No additional comment	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
We support the interpretation. It is our belief that NERC and the regions continue to focus on the Registered Entity's ability to self-determine BES Cyber Systems and shared BES Cyber Systems. We support the direction to the guidance in the background section of CIP-002-5.1 that states: "it is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System".	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
We agree with the response to Question 1.	

Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	
Reclamation believes that examples would be helpful for understanding the scope of EnergySec's request and the NERC response.	
Likes 0	
Dislikes 0	
Response	

2. Do you agree with the response to Question 2? If not please provide the basis for your disagreement and an alternate proposal.

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

2. Initial ballot for CIP-003-7 Implementation Plan

Vote: No

Comments: PacifiCorp supports comments submitted by Edison Electric Institute. Also, the language in the definitions and CIP-003-7 currently out for vote is a substantial rewrite of the requirements as approved by FERC. PacifiCorp cannot afford to wait to begin implementation until a revised standard is approved by FERC, meaning that any approved version that does not allow PacifiCorp to leverage work efforts already completed in alignment with the current FERC approved standard would lead to duplicative effort and costs. Any attempt to compress the overall timeline for implementation could results in a negative impact to the reliability of the bulk electric system

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	No
Document Name	

Comment

We incorporate our response to Question No. 1.

The object of “those,” like at, “…are those shared…” may seem ambiguous, but the plain reading of the sentence in context illustrates “those” refers to generating units. Substituting “generating units” for “those,” the sentence reads:

“For each group of generating units, the only BES Cyber Systems that meet this criterion are **generating units** shared BES Cyber Systems that could, within 15 minutes…”

This supports the SDT’s proposed interpretation—that all the generating units share the discrete BES Cyber Systems. However, as discussed in our response to Question 1, we believe the path to clarifying the ambiguous and uncertain language requires revision of Criterion 2.1 and the underlying Standard. The material revisions required to resolve the issues cannot be gained through the interpretation process.

Likes 0	
Dislikes 0	

Response	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Jaclyn Massey - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	
Response	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
However, this does not resolve the question of what is "discreet"	
Likes 0	
Dislikes 0	
Response	

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees that the phrase "shared BES Cyber Systems" applies to discrete BES Cyber Systems ahred by mutliple generators within a generation facility. SCE notes that this term was clarified in the NERC Frequently Asked Questions (FAC) No. 49.	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	
Reclamation believes that examples would be helpful for understanding the scope of EnergySec's request and the NERC response.	
Likes 0	
Dislikes 0	
Response	

3. Do you agree with the response to Question 3? If not please provide the basis for your disagreement and an alternate proposal.

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

In response to Question #2, the drafting team determined, “The phrase ‘shared BES Cyber Systems’ refers to discrete BES Cyber Systems…*shared by multiple generation units*.” (emphasis added)

Accordingly, Question #3 seeks guidance regarding how to determine if BES Cyber Systems are “shared” by generation units so as to fall into Criterion 2.1. The proposed response does not do so. Again, AE *believes* the drafting team intended to say:

CIP-002-5.1 contains no guidance regarding how to *group* BES Cyber Systems to determine their impact on generation units aggregating ≥ 1500 MW. Accordingly, Responsible Entities have discretion regarding whether or how to “group” BES Cyber Systems. Consequently, a Compliance Enforcement Authority has no basis for questioning a Responsible Entity’s conclusions regarding whether or how to group BES Cyber Systems with respect to their ability to adversely impact the reliable operation of generation units aggregating to ≥ 1500 MW in a single Interconnection.

If AE has interpreted the proposed response correctly, the drafting team should clearly make that statement. If AE is not correct, the drafting team should rewrite the response to make it clearer.

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3

Answer	No
Document Name	

Comment

What is the defintition of "discreet"? What attributes make a system discreet?

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	No

Document Name	
Comment	
We incorporate our response to Question No. 1 and its proposed path forward.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
3. Initial ballot for the new term - Low Impact External Routable Communication (LERC) and its definition Vote: No Comments: PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets	
Likes 0	
Dislikes 0	
Response	
Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees that the phrase applies to each discrete BES Cyber System, rather than collectively to groups of BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Jaclyn Massey - Entergy - Entergy Services, Inc. - 5	

Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
ACES supports that the phrase applies to each discrete BES Cyber Systems. While we understand the RFI was limited to "shared," we would like the interpretation team to consider issuing guidance on jointly-owned BES Cyber Systems regarding where and how responsibility, compliance and auditability applies to each owner.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	
Reclamation believes that examples would be helpful for understanding the scope of EnergySec's request and the NERC response.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)
Comment Period Start Date:	7/27/2016
Comment Period End Date:	9/12/2016
Associated Ballots:	2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec) CIP-002-5.1 IN 1 INT

There were 18 sets of responses, including comments from approximately 49 different people from approximately 42 companies representing 8 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

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 Director of Standards Development, Steve Noess (via email) or at (404) 446-9691.

Questions

1. Do you agree with the response to Question 1? If not, please provide the basis for your disagreement and an alternate proposal.

2. Do you agree with the response to Question 2? If not please provide the basis for your disagreement and an alternate proposal.

3. Do you agree with the response to Question 3? If not please provide the basis for your disagreement and an alternate proposal.

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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC

					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					Brian Shanahan	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Quintin Lee	Eversource Energy	1	NPCC

					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Sean Bodkin	Dominion	4	NPCC
ACES Power Marketing	Warren Cross	1,3,5,6	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Brazos Electric Power Cooperative, Inc.	BREC	1,5	Texas RE
					Prairie Power, Inc.	PPI	1,3	SERC
					Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF

					East Kentucky Power Cooperative	EKPC	1,3	SERC
					Sunflower Electric Power Corporation	SEPC	1	SPP RE
					Great River Energy	GRE	1,3,5,6	MRO

1. Do you agree with the response to Question 1? If not, please provide the basis for your disagreement and an alternate proposal.	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	

As Austin Energy (AE) understands the question, EnergySec is asking whether the entity must determine:

1. Whether each discrete BES Cyber System "could, within 15 minutes, adversely impact the reliable operation" of generation units aggregating to ≥ 1500 MW; ***or***

2. Whether, collectively, groups of BES Cyber Systems at the generation facility "could, within 15 minutes, adversely impact the reliable operation" of generation units aggregating to ≥ 1500 MW.

The proposed response merely regurgitates the contents of the Background discussion regarding an entity's freedom to group BES Cyber Assets into BES Cyber Systems, it does not answer the question of how to determine if BES Cyber Systems are ***shared***.

AE *believes* the drafting team intended to say:

CIP-002-5.1 contains no *requirement* to *group* BES Cyber Systems. Accordingly, Responsible Entities may determine whether to consider BES Cyber Systems "shared." Consequently, a Compliance Enforcement Authority has no basis for questioning a Responsible Entity's conclusions regarding whether BES Cyber Systems are "shared" with respect to their ability to adversely impact the reliable operation of generation units aggregating to ≥ 1500 MW in a single Interconnection.

If AE has interpreted the proposed response correctly, the drafting team should clearly say so. If AE is not correct, the drafting team should rewrite the response to make it clearer.

Likes 0	
Dislikes 0	

Response: Thank you for your comments.

1. The IDT responded to the request for interpretation as submitted and reiterates that, consistent with the interpretation response to Question 2, the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units."
2. The response to Question 2 further states quoting FAQ #49 "Shared BES Cyber Systems are those that are associated with any combination of units in a single interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2."

It is by analysis of the BES Cyber Systems impact, not simply entity discretion, that a determination of "shared" is reached.

Diana McMahon - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP does not agree that the answer provided addresses the question. The question is not if an evaluation is to be done to determine if a BES Cyber system is shared. SRP understands the question to be asking whether the criterion should be performed on a discrete BES Cyber System shared by multiple generating units at a single plant location or on a collection of BES Cyber Systems shared by multiple generating units at a single plant location.

Likes 0	
Dislikes 0	

Response: Thank you for your comment.

The IDT response clearly states that "in the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems."

John Hagen - Pacific Gas and Electric Company - 3

Answer	No

Document Name	
Comment	
Logical grouping of assets should be at the discretion of the entity and not a requirement However, this ambiguity may not be supported at audit	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The IDT agrees that the grouping of BES Cyber Assets is at the discretion of the Responsible Entity. This is supported by the discussion in the Background section of CIP-002-5.1 which states "it is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The discretion of grouping BES Cyber Assets into BES Cyber Systems was not questioned in the interpretation.	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
We disagree that evaluation of each BES Cyber System needs to be performed individually for each discrete BES Cyber System. The question may be addressed by simply looking at the elements that comprise Criterion 2.1. **The Elements of Criterion 2.1 are:** Generation	

- Commissioned generation
- A group [which we interpret as 1 or more] generating units
- The generating units are at a single plant location
- The generating units aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceed 1500 MW
- The 1500MW threshold is at a single Interconnection.

Relationship Between the Generation and the BES Cyber Systems

- The generating units share a BES Cyber System

The BES Cyber System

- The BES Cyber System can cause an adverse impact to the reliable operation of any combination of the generating units
- The adverse impact is within 15 minutes
- The aggregate adverse impact equals or exceeds 1500 MW
- The 1500MW adverse impact occurs at a single Interconnection.

In consideration of the criteria, if a single element is false / untrue, the BES Cyber System does not meet the threshold of a Medium Impact Risk. While we think that is straight forward, there is some nuance associated with the evaluation of a BES Cyber System, which is likely the genesis of the question.

The evaluation of a BES Cyber System.

The question asked for clarification of the term BES Cyber Systems, wanting to know if it means each individual and discrete BES Cyber System at a single plant location or collectively for groups of BES Cyber Systems.

We think clarification is found in Criterion 2.1 elements. For example, if there is a group of BES Cyber Systems and evaluation of the individual components determine the Criterion 2.1 thresholds are not met. At that point, it would be easy to say they are not a Medium Impact Risk. However, Criterion 2.1 language, paraphrased, is BES Cyber Systems that *could* adversely impact reliable operation of the generation units.

We feel the "could" qualifier brings into scope the relationship between and reliance upon the individual components of the group of BES Cyber Systems.

In other words:

If there is a failure in the interaction between two of the multiple BES Cyber Systems.

AND

The failure between the BES Cyber Systems "…within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection,"

AND

All other elements of Criterion 2.1 are met.

THEN

The threshold is pierced and the Medium Impact Risk is assigned.

It is Not Necessary to Evaluate Each Individual BES Cyber System

Based on the example, it may not be necessary to evaluate each individual BES Cyber System if the Criterion 2.1 threshold is breached on the potential failure of the interaction between two BES Cyber Systems.

We recognize the Criterion is specific to BES Cyber Systems and not the interaction between systems, but the "could" qualifier brings those interactions into scope of the evaluation regardless whether the individual BES Cyber System, alone, can cause the requisite adversity to reliability.

Resolution is Found in the Standard Revision Process

We believe the path to clarifying the ambiguous and uncertain language requires revision of Criterion 2.1 and the underlying Standard. The material revisions required to resolve the issues cannot be gained through the interpretation process.

Jointly-Owned Units Not Considered in Standard

Of additional concern are scenarios of jointly owned units (JOU) with BES Cyber Systems that communicate between entities and also meet Criterion 2.1. While contracts will delineate owners' responsibilities, it is common with JOU a level of parallel systems that, individually, "could" pierce the adverse reliability threshold.

Likes 0	
Dislikes 0	

Response: Thank you for your comments.

The IDT agrees with the comment that a single impact analysis may apply to the categorization of multiple BES Cyber Systems. For instance, if multiple BES Cyber Systems support a generation resource which totals only 500 MW in capability, then none of those BES Cyber Systems are associated with "commissioned generation…with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection." (CIP-002-5.1 Attachment 1, Criterion 2.1) However, the IDT asserts that the categorization of those individual BES Cyber Systems is still completed discretely, despite reliance on a single analysis of the total megawatt output capability of the generation resource.

Regarding the question of the interaction between two BES Cyber Systems, the determination of impact level is dependent upon the facts and circumstances surrounding the BES Cyber System in question. These facts and circumstances must be evaluated in the assessment to determine the impact level of the BES Cyber System. It is outside the scope of an interpretation to determine or assess the facts and circumstances for a specific scenario.

Consistent with the response to the interpretation and the obligations outlined in CIP-002-5.1, a Responsible Entity must evaluate criterion 2.1 in the context of shared BES Cyber Systems. "The phrase 'shared BES Cyber Systems' refers to discrete BES Cyber Systems that are shared by multiple generation units." (EnergySec CIP-002-5.1 Interpretation Response, Question 2)

Regarding the question of jointly-owned units, that issue was not the subject of the interpretation request. A separate Request for interpretation (RFI) or Standard Authorization Revision (SAR) may be submitted to raise the questions of jointly-owned units.

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
1. Initial ballot for CIP-003-7 - Cyber Security – Security Management Controls Vote: No Comments: PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The IDT noticed that these comments are the same as those submitted for Project 2016-02 LERC posting and they are responsive to that proposal. The SDT will address the concerns in response to the initial LERC posting rather than for the EnergySec Interpretation of CIP-002-5.1.	
Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SCE agrees that a BES Cyber System that is shared between multiple generators needs to be evaluated individually, as opposed to being collectively grouped. Furthermore, SCE agrees that there is no obligation to group BES Cyber Systems. Each entity is given the choice of granularity in grouping BES Cyber Assets into BES Cyber Systems, but is not required to group BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments.	
Jaclyn Massey - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
No additional comment	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	

We support the interpretation. It is our belief that NERC and the regions continue to focus on the Registered Entity's ability to self-determine BES Cyber Systems and shared BES Cyber Systems. We support the direction to the guidance in the background section of CIP-002-5.1 that states:

"it is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System".

Likes 0	
Dislikes 0	

Response: Thank you for your comments.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC

Answer	Yes
Document Name	

Comment

We agree with the response to Question 1.

Likes 0	
Dislikes 0	

Response: Thank you for your comment.

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 5	

Answer	
Document Name	
Comment	
Reclamation believes that examples would be helpful for understanding the scope of EnergySec's request and the NERC response.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. No such examples were submitted to the IDT as part of the request for interpretation and the IDT is limited from discussing specific compliance approaches. Other venues exist to explore applicable examples such as NERC's Implementation Guidance process.	

2. Do you agree with the response to Question 2? If not please provide the basis for your disagreement and an alternate proposal.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
2. Initial ballot for CIP-003-7 Implementation Plan Vote: No Comments: PacifiCorp supports comments submitted by Edison Electric Institute. Also, the language in the definitions and CIP-003-7 currently out for vote is a substantial rewrite of the requirements as approved by FERC. PacifiCorp cannot afford to wait to begin implementation until a revised standard is approved by FERC, meaning that any approved version that does not allow PacifiCorp to leverage work efforts already completed in alignment with the current FERC approved standard would lead to duplicative effort and costs. Any attempt to compress the overall timeline for implementation could results in a negative impact to the reliability of the bulk electric system	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The IDT noticed that these comments are the same as those submitted for Project 2016-02 LERC posting and they are responsive to that proposal. The SDT will address the concerns in response to the initial LERC posting rather than for the EnergySec Interpretation of CIP-002-5.1.	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No

Document Name	
Comment	
We incorporate our response to Question No. 1. The object of “those,” like at, “…are those shared…” may seem ambiguous, but the plain reading of the sentence in context illustrates “those” refers to generating units. Substituting “generating units” for “those,” the sentence reads: “For each group of generating units, the only BES Cyber Systems that meet this criterion are **generating units** shared BES Cyber Systems that could, within 15 minutes…” This supports the SDT’s proposed interpretation—that all the generating units share the discrete BES Cyber Systems. However, as discussed in our response to Question 1, we believe the path to clarifying the ambiguous and uncertain language requires revision of Criterion 2.1 and the underlying Standard. The material revisions required to resolve the issues cannot be gained through the interpretation process.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The IDT disagrees that “those” refers to generating units; and asserts that “those” refers to “shared BES Cyber Systems.” (CIP-002-5.1 Attachment 1, Criterion 2.1) The IDT disagrees that modification of CIP-002-5.1 Attachment 1, Criterion 2.1 is necessary.	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	

No comments.	
Likes 0	
Dislikes 0	
Response	
Jaclyn Massey - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	
Response	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
However, this does not resolve the question of what is "discreet"	
Likes 0	

Dislikes 0	
Response: Thank you for your comments. Question 2 asks “whether the phrase ‘shared BES Cyber Systems’ refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units.” The IDT responded that “the phrase ‘shared BES Cyber Systems’ refers to discrete BES Cyber Systems that are shared by multiple generation units.” The definition of “discrete” was not raised in this interpretation and the IDT contends that the meaning of “discrete” is clear in this context.	
Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees that the phrase "shared BES Cyber Systems" applies to discrete BES Cyber Systems ahred by mutliple generators within a generation facility. SCE notes that this term was clarified in the NERC Frequently Asked Questions (FAC) No. 49.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments.	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Erika Doot - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	
Reclamation believes that examples would be helpful for understanding the scope of EnergySec's request and the NERC response.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. No such examples were submitted to the IDT as part of the request for interpretation and the IDT is limited from discussing specific compliance approaches. Other venues exist to explore applicable examples such as NERC's Implementation Guidance process.	

3. Do you agree with the response to Question 3? If not please provide the basis for your disagreement and an alternate proposal.	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	

In response to Question #2, the drafting team determined, "The phrase 'shared BES Cyber Systems' refers to discrete BES Cyber Systems…*shared by multiple generation units*." (emphasis added)

Accordingly, Question #3 seeks guidance regarding how to determine if BES Cyber Systems are "shared" by generation units so as to fall into Criterion 2.1. The proposed response does not do so. Again, AE *believes* the drafting team intended to say:

CIP-002-5.1 contains no guidance regarding how to *group* BES Cyber Systems to determine their impact on generation units aggregating ≥ 1500 MW. Accordingly, Responsible Entities have discretion regarding whether or how to "group" BES Cyber Systems. Consequently, a Compliance Enforcement Authority has no basis for questioning a Responsible Entity's conclusions regarding whether or how to group BES Cyber Systems with respect to their ability to adversely impact the reliable operation of generation units aggregating to ≥ 1500 MW in a single Interconnection.

If AE has interpreted the proposed response correctly, the drafting team should clearly make that statement. If AE is not correct, the drafting team should rewrite the response to make it clearer.

Likes 0	
Dislikes 0	

Response: Thank you for your comments.

As written, Question 3 asks specifically about the grouping of shared BES Cyber Systems. The IDT responded that "the phrase [shared BES Cyber Systems] applies to each discrete BES Cyber System."

Additionally, please see the IDT response to Austin Energy's comments in Question 1.

John Hagen - Pacific Gas and Electric Company - 3	
Answer	No
Document Name	
Comment	
What is the defintition of "discreet"? What attributes make a system discreet?	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The definition of “discrete” was not raised in this interpretation.	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
We incorporate our response to Question No. 1 and its proposed path forward.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
3. Initial ballot for the new term - Low Impact External Routable Communication (LERC) and its definition Vote: No Comments: PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The IDT noticed that these comments are the same as those submitted for Project 2016-02 LERC posting and they are responsive to that proposal. The SDT will address the concerns in response to the initial LERC posting rather than for the EnergySec Interpretation of CIP-002-5.1.	
Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees that the phrase applies to each discrete BES Cyber System, rather than collectively to groups of BES Cyber Systems.	

Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Jaclyn Massey - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
ACES supports that the phrase applies to each discrete BES Cyber Systems. While we understand the RFI was limited to "shared," we would like the interpretation team to consider issuing guidance on jointly-owned BES Cyber Systems regarding where and how responsibility, compliance and auditability applies to each owner.	

Likes 0	
Dislikes 0	
Response: Thank you for your comment. Regarding the question of jointly-owned units, that issue was not the subject of the interpretation request. A separate Request for interpretation (RFI) or Standard Authorization Revision (SAR) may be submitted to raise the questions of jointly-owned units.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michelle Amarantos - APS - Arizona Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	
Reclamation believes that examples would be helpful for understanding the scope of EnergySec's request and the NERC response.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. No such examples were submitted to the IDT as part of the request for interpretation and the IDT is limited from discussing specific compliance approaches. Other venues exist to explore applicable examples such as NERC's Implementation Guidance process.	

Appendix 1

Interpretation of CIP-002-5.1, Requirement R1, Attachment 1, Criterion 2.1

Requirement Number and Text of Requirement
<u>CIP-002-5.1, Requirement R1</u> R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required). <u>Attachment 1, Criterion 2.1</u> 2. Medium Impact Rating (M) Each BES Cyber System, not included in Section 1 above, associated with any of the following: 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions
Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems." The Interpretation Drafting Team identified the following questions in the RFI: 1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems? 2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units? 3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?
Responses
Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems? The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added) Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides: > 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.

Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec)

Final Ballot Open through October 24, 2016

Now Available

A 10-day final ballot for the **Interpretation of CIP-002-5.1** is open through **8 p.m. Eastern, Monday, October 24, 2016**.

Balloting

In the final ballot, votes are counted by exception. Only members of the ballot pool may cast a vote. All ballot pool members may change their previously cast vote. A ballot pool member who failed to vote during the previous ballot period may vote in the final ballot period. If a ballot pool member does not participate in the final ballot, the member's vote from the previous ballot will be carried over as their vote in the final ballot.

Members of the ballot pool associated with this project may log in and submit their vote for the interpretation here. If you experience any difficulties using the Standards Balloting & Commenting System (SBS), contact Nasheema Santos.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

The voting results for the interpretation will be posted and announced after the ballot closes. If approved, the interpretation will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Ballot Name: 2015-INT-01 Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec) CIP-002-5.1 FN 2 INT
Voting Start Date: 10/13/2016 10:39:23 AM
Voting End Date: 10/24/2016 8:00:00 PM
Ballot Type: INT
Ballot Activity: FN
Ballot Series: 2
Total # Votes: 234
Total Ballot Pool: 288
Quorum: 81.25
Weighted Segment Value: 91.31

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	70	1	41	0.953	2	0.047	0	14	13
Segment: 2	7	0.2	2	0.2	0	0	0	3	2
Segment: 3	62	1	33	0.868	5	0.132	0	12	12
Segment: 4	19	1	13	0.929	1	0.071	0	4	1
Segment: 5	70	1	36	0.857	6	0.143	0	11	17

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 6	46	1	24	0.828	5	0.172	0	8	9
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	1	0.1	0	0	0	1	0
Segment: 10	9	0.9	9	0.9	0	0	0	0	0
Totals:	288	6.5	162	5.935	19	0.565	0	53	54

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		Affirmative	N/A
1	Bonneville Power Administration	Donald Watkins		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Abstain	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Shawna Speer		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		None	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro-Qu?bec Production	Aviance Freeman		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Abstain	N/A
1	JEA	Ted Hobson	Joe McClung	None	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Abstain	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.0 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Abstain	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A
1	Salt River Project	Steven Cobb		Negative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Abstain	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Jennifer Wright	Harold Sherrill	Abstain	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		None	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Abstain	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Abstain	N/A
1	Westar Energy	Kevin Giles		None	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		None	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Midcontinent ISO, Inc.	Terry BIlke		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Michael DeLoach		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Black Hills Corporation	Eric Egge		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		None	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Abstain	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Abstain	N/A
3	Gainesville Regional Utilities	Ken Simmons		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	N/A
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		None	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Ocala Utility Services	Randy Hahn		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Abstain	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Negative	N/A
3	Platte River Power Authority	Jeff Landis		None	N/A
3	PNM Resources	Michael Mertz		None	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		Negative	N/A
3	Puget Sound Energy, Inc.	Andrea Basinski		Abstain	N/A
3	Salt River Project	Rudy Navarro		Negative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Abstain	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERGDVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Mark Oens		Abstain	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		None	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Abstain	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		None	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Austin Energy	Tina Garvey		Negative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		Affirmative	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		Affirmative	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Abstain	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Abstain	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Abstain	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Matthew Finn		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	Black Hills Corporation	George Tatar		Negative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Bonneville Power Administration	Francis Halpin		None	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Negative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Abstain	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough		Abstain	N/A
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Abstain	N/A
5	Muscatine Power and Water	Mike Avesing		Abstain	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Wayne Sipperly		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Leo Staples		Negative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Abstain	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer		Abstain	N/A
5	Salt River Project	Kevin Nielsen		Negative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Abstain	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		None	N/A
5	U.S. Bureau of Reclamation	Erika Doot		Abstain	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		None	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Negative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	N/A
6	Bonneville Power Administration	Andrew Meyers		None	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Negative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Entergy	Julie Hall		None	N/A
6	Exelon	Maggy Powell		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Abstain	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Abstain	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Negative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		None	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
6	N.S. Machine Name Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A

© 2016 - NERC Ver 3.0.1.6 - Machine Name: ERODVSBSWB01

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Abstain	N/A
6	Platte River Power Authority	Sabrina Martz		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		None	N/A
6	Salt River Project	Chris Janick		Negative	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Affirmative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Abstain	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Abstain	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 288 of 288 entries

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

© 2016 - NERC Ver 3.0.1.6 Machine Name: ERODVSBSWB01

Exhibit C

Interpretation Drafting Team Roster

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team Roster

Project 2016-02 Modifications to CIP Standards

	Name	Entity
Chair	Margaret Powell	Exelon
Vice Chair	Christine Hasha	Electric Reliability Council of Texas
Vice Chair	David Revill	Georgia Transmission Corporation
Members	Steven Brain	Dominion
	Jay Cribb	Southern Company
	Jennifer Flandermeyer	Kansas City Power and Light
	Tom Foster	PJM Interconnection
	Richard Kinas	Orlando Utilities Commission
	Forrest Krigbaum	Bonneville Power Administration
	Philippe Labrosse	Hydro-Quebec TransEnergie
	Mark Riley	Associated Electric Cooperative, Inc.