UNITED STATES OF AMERICA
Before the
FEDERAL ENERGY REGULATORY COMMISSION

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

STATUS REPORT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO THE FEDERAL ENERGY REGULATORY COMMISSION'S MARCH 19, 2009 ORDER No. 706-B

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

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

October 15, 2010

TABLE OF CONTENTS

ATTACHMENTS:

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") respectfully submits this status report in response to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Order No. 706-B issued on March 19, 2009.[1] In Order No. 706-B, the Commission clarified that facilities within a nuclear generation plant in the United States are subject to compliance with the eight mandatory Critical Infrastructure Protection ("CIP") Reliability Standards. The Commission therefore directed NERC, as the Electric Reliability Organization ("ERO"), to assure that there is no "gap" in the regulatory process by determining whether the "balance of plant" equipment within a nuclear power plant in the United States that is not regulated by the NRC is subject to compliance with the CIP Reliability Standards approved in Order No. 706.[2]

In determining that "all balance of equipment within a nuclear power plant is subject to the CIP Reliability Standards," the Commission also noted that "a nuclear power plant licensee may seek an exception from the ERO to the extent that the licensee believes that specific equipment within the balance of plant is subject to NRC cyber security regulations."[3] The Commission stated that "subjecting all balance of plant equipment within a nuclear power plant to the CIP Reliability Standards, with exceptions allowed via a process implemented by the ERO, nuclear power plant licensees will have a bright-line rule that eliminates a potential regulatory gap and provides certainty; and a plant-specific equipment exception process to avoid dual regulation where appropriate."[4] Accordingly, NERC was directed to determine the "bright-

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 126 FERC ¶61,220 (Order No. 706-B) (March 19, 2009).
[2] *Id.* at P 1.
[3] *Id.* at PP 49 and 50.
[4] *Id.* at P 50.

line" for nuclear power plants in accordance with the Commission's guidance in Order No. 706-B.

The timetable for determining the "bright-line" criteria regarding whether a nuclear power plant's balance of plant equipment is subject to compliance with NERC CIP Reliability Standards or with the NRC cyber security regulations was determined based on the CIP-002 through CIP-009 implementation timetable for nuclear power plants, which was submitted for FERC approval by NERC on January 19, 2010. That Implementation Plan is structured such that the timeline for compliance with each requirement within the CIP Reliability Standards is the later of: (i) the FERC-approved effective date of the Implementation Plan plus 18 months (*i.e.*, the "R" date in the proposed CIP Version 1 Implementation Plan); the date the scope of systems determination is completed plus 10 months (*i.e.*, the "S" date in the proposed CIP Version 1 Implementation Plan); or (iii) if an outage is required for implementation of certain requirements, six months following the completion of the first refueling outage at least 18 months following the FERC effective date of the Implementation Plan.

On March 18, 2010, FERC approved NERC's implementation timetable for nuclear power plants.[5] Accordingly, NERC hereby submits this status report to address the status of the preliminary scope of systems (bright-line) determination and explains next steps being taken to finalize the scope of systems determination in order to assess nuclear power plants' timing and compliance obligations regarding the NERC CIP Reliability Standards.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this status report may be addressed to:

[5] *Order Addressing Compliance Filing and Approving Implementation Plan,*130 FERC ¶ 61,185 (March 18, 2010).

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

* Persons to be included on FERC's service list are indicated with an asterisk. NERC requests waiver of FERC's rules and regulations to permit the inclusion of more than two people on the service list.

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

III. STATUS OF ORDER NO. 706-B BRIGHT LINE DETERMINATION

In Order No. 706-B, FERC directed NERC to conduct an analysis of nuclear power plant balance of plant systems to determine which of those systems should be subject to compliance with the NERC CIP Reliability Standards. Specifically, FERC stated in Order No. 706-B that a nuclear power plant licensee may seek an exception to CIP Reliability Standard compliance if it believes that specific equipment within the balance of plant is subject to NRC cyber security regulations.[6] FERC stated that it "would expect that the ERO would make such determinations with the consultation of NRC and oversight of Commission staff."[7]

As part of these efforts, on December 30, 2009, NERC and the NRC executed a Memorandum of Understanding to address NERC and the NRC's processes for soliciting information from nuclear power plants in order to determine which systems, structures, and

[6] Order No. 706-B at P. 50.
[7] *Id.*

components ("SSCs") may be exempted from compliance with NERC CIP Reliability Standards.[8]

NERC and the NRC held four workshops in Charlotte, Phoenix, Philadelphia, and Chicago in April and May 2010 to discuss NERC and the NRC's efforts to delineate which of the nuclear power plant SSCs are subject to compliance with the NERC CIP Reliability Standards, and which are subject to compliance with the NRC cyber security regulations. In advance of these workshops, NERC issued a draft Section 1600 data request, in accordance with Section 1600 of the NERC Rules of Procedure,[9] to all nuclear power plants in the United States requesting each NPP to delineate its balance of plant SSCs subject to the NRC cyber security regulations (10 C.F.R. §73) and those subject to compliance with NERC CIP Reliability Standards for discussion at the workshops. All of the 104 Nuclear Power Plants in the United States were represented at the workshops. Therefore, all Nuclear Power Plants had an opportunity to discuss the draft survey with NERC and NRC staff. The draft survey was posted for public comment from May 19, 2010 to June 2, 2010. There were a total of 13 comments received, and minor modifications were made to the survey as a result.

On June 14, 2010, NERC sent the final version of the Section 1600 data request to each nuclear power plant in the United States. The survey was developed by the NRC and NERC in order to preliminarily determine those SSCs subject to compliance with NERC CIP Reliability Standards (listed in Attachment I of the survey) and those subject to NRC cyber security regulations (listed in Attachment II of the survey). In responding to the survey, nuclear power plants were specifically given an opportunity to state whether any of their balance of plant systems should not be subject to compliance with the NERC CIP Reliability Standards because

[8] The MOU is available at: http://www.nerc.com/files/MOU_Final.pdf.
[9] NERC's Rules of Procedure are available at: http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20100903.pdf.

they were instead subject to compliance with the NRC cyber security regulations. The June 14 survey is included as **Attachment A** to this filing. All 104 NPPs in the United States responded to the Section 1600 survey, stating that all of their balance of plant SSCs are subject to NRC cyber security regulations.

After consultation with the NRC, on August 27, 2010, NERC sent a letter to each NPP in response to their completed surveys. The letter is included as **Attachment B** to this filing. In the letter, NERC notified the nuclear power plants that, in order to verify that the balance of plant SSCs are covered under the NRC's jurisdiction and therefore not subject to NERC jurisdiction, each nuclear power plant must provide the NRC a notification letter identifying all balance of plant SSCs that are considered "important to safety" and therefore subject to NRC cyber security requirements.

All of the 104 nuclear power plants in the United States responded to the August 27, 2010 letter confirming that all balance of plant SSCs at their respective plants are "important to safety" and therefore subject to the NRC's cyber security requirements.

Because all nuclear power plants have submitted a notification letter to the NRC, with a copy to NERC, stating that all of their balance of plant SSCs are subject to NRC cyber security regulations, NERC has preliminarily determined (*i.e.,* the "Scope of Systems" or "bright-line" determination) that these SSCs ***are not*** subject to compliance with NERC CIP Reliability Standards in accordance with Order No. 706-B. However, because the NRC must still confirm the nuclear power plant's determinations that all of their balance of plant SSCs are subject to NRC cyber security regulations, NERC cannot now set a final "Scope of Systems Determination" (*i.e.,* "bright-line") date. Accordingly, NERC will make another filing to FERC

within thirty (30) days of the NRC's final determination to report on the status of this final determination.

In coordination with the NRC, with consideration of the information provided by the Nuclear Energy Institute (NEI), and with oversight from FERC, NERC has completed a gap analysis of the NERC CIP Reliability Standards and the NRC's physical and cyber security controls. The gap analysis concluded the NRC controls are equal to or better than the NERC CIP standards. The "NRC/NERC Security Standards Gap Analysis" is included as **Attachment C** to this filing.

As noted, the "Scope of Systems" or "bright-line" date will become final upon the NRC's confirmation that the SSCs declared by the nuclear power plants to be subject to NRC cyber security regulations are, in fact, so. If the NRC determines that these balance of plant SSCs are not within the scope of its jurisdiction, these SSCs will be subject to compliance with the applicable NERC CIP Reliability Standards. Within thirty (30) days of the NRC's final confirmation regarding whether the nuclear power plants' SSC's are subject to NRC cyber security regulations, NERC will submit an informational filing to FERC regarding the status of nuclear power plants under the CIP Reliability Standards and any necessary next steps to be taken in this proceeding.

IV. CONCLUSION

NERC respectfully requests that FERC accept this status report and Attachments regarding FERC's directive in Order No. 706-B to establish the scope of systems ("bright-line") determination for nuclear power plants' compliance with the mandatory NERC CIP Reliability Standards.

Respectfully submitted,

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

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

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 15th day of October, 2010.

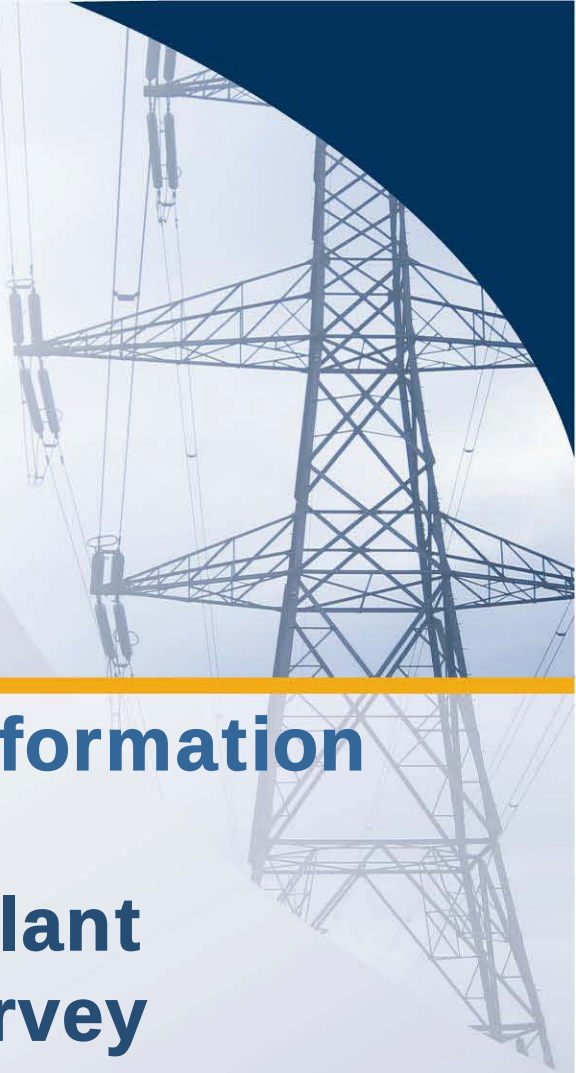
/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney for North American Electric Reliability Corporation

ATTACHMENT A

June 14, 2010 NERC Section 1600 Survey to Nuclear Power Plants

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



Request for Data or Information

Nuclear Power Plant "Bright-Line" Survey

to ensure the reliability of the bulk power system

Bright-Line Survey
June 11, 2010

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

Table of Contents

Introduction and Survey Scope

In accordance with Section 1600 of the NERC Rules of Procedure,[1] NERC may request data or information that is deemed necessary to meet its obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d) of the Federal Energy Regulatory Commission's ("FERC") regulations. This is a proposal for such a request. Section 1606 of the NERC Rules of Procedure allows for a shortened time period for posting a request for data or information if the data or information must be obtained in order to comply with a directive in an order issued by FERC or another governmental authority. In Order No. 706-B,[2] FERC directed NERC to conduct an analysis of Nuclear Power Plant ("NPP") balance of plant ("BOP") systems in order to determine those systems that should be subject to the NERC Critical Infrastructure Protection ("CIP") Reliability Standards (the "bright-line" determination). Accordingly, NERC is issuing this request for data or information in accordance with the timing requirements of Section 1606 of the NERC Rules of Procedure. NERC provided this proposed data request to FERC for information on May 14, 2010. On May 18, 2010, the NERC Board of Trustees authorized the shortened comment period. NERC is hereby posting this proposed data request for public comment for a fourteen (14) day comment period. After consideration of comments received, NERC will present this proposed data request to the NERC Board of Trustees for approval, as required by Section 1602 of the NERC Rules of Procedure. Upon NERC Board of Trustees approval, this data request will become mandatory.

The purpose of this survey is to solicit data and information from each NPP in the United States regarding their systems, structures, and components ("SSCs") in order to determine whether those SSCs may be required to comply with applicable NERC CIP Reliability Standards in accordance with Section 215 of the Federal Power Act (FPA) and the FERC Order Approving the CIP Version 1 Implementation Plan for NPP Owners and Operators.[1] FERC Order No. 706-B found that the NRC regulations on cyber security would not apply to all SSCs within an NPP and therefore the remaining BOP SSCs may be subject to compliance with the applicable NERC CIP Reliability Standards.[2]

As a result of Order No. 706-B and the December 30, 2009 NERC and NRC Memorandum of Understanding (MOU),[3] which addresses NERC and the NRC's processes for soliciting information from NPPs in order to determine which SSCs may be exempted from compliance with NERC CIP Reliability Standards, NERC, in coordination with the NRC, has developed a generic list of SSCs that may be subject to the NERC CIP Reliability Standards (**Attachment I**). **Attachment II** includes a generic list of SSCs that are potentially subject to NRC Cyber Security Regulations and therefore excluded from compliance with NERC CIP Reliability Standards. Because these are generic lists, it is essential that each NPP provide NPP-specific responses to this survey.

[1] NERC's Rules of Procedure are available at: http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20100121.pdf

[2] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706-B, 126 FERC ¶ 61,229 (2009) ("Order No. 706-B").

[3] The MOU is available at: http://www.nerc.com/files/MOU_Final.pdf

Due Date and NERC Contact Information

The completion of this survey and submission to NERC is due within thirty days after receipt of the survey.

Please email the completed survey with applicable attached documentation to Jim Hughes at: Jim.Hughes@nerc.net. If any of your responses to this survey are deemed confidential/safeguards, please contact Jim Hughes directly for further instructions.

Any other questions may be directed to Jim Hughes at the email provided above or by telephone at 609.203.2288.

The completed survey may also be mailed to:

NERC
C/O Jim Hughes, Senior Auditor
116 - 390 Village Boulevard
Princeton, New Jersey 08540

Alternate NERC Points of Contact:

Tim Roxey: Tim.Roxey@nerc.net
Phone: 410.474.9240.

Monica Benson: Monica.Benson@nerc.net
Phone: 609.524.7073.

Authority

Under Section 215 of the Federal Power Act (16 U.S.C. § 824o), Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the Nation's bulk power system, and with the duties of certifying an Electric Reliability Organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to FERC approval. NERC was certified as the ERO on July 20, 2006. NERC's authority for issuing this survey is derived from Section 215 of the Federal Power Act, and from the following sources:

NERC is requesting this information in accordance with its authority provided in 18 C.F.R. §39.2(d), which provides:

> *Each user, owner or operator of the Bulk-Power System within the United States (other than Alaska and Hawaii) shall provide the Commission, the Electric Reliability Organization and the applicable Regional Entity such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission and set out in the Rules of the Electric Reliability Organization and each applicable Regional Entity. The Electric Reliability Organization and each Regional Entity shall provide the Commission such information as is necessary to implement section 215 of the Federal Power Act.*

Additionally, NERC Rules of Procedure Section 1600 provides:

> ***1601. Scope of a NERC or Regional Entity Request for Data or Information***
> *Within the United States, NERC and regional entities may request data or information that is necessary to meet their obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d) of the Commission's regulations, 18 C.F.R. § 39.2(d). In other jurisdictions NERC and regional entities may request comparable data or information, using such authority as may exist pursuant to these rules and as may be granted by ERO governmental authorities in those other jurisdictions. The provisions of Section 1600 shall not apply to requirements contained in any Reliability Standard to provide data or information; the requirements in the Reliability Standards govern. The provisions of Section 1600 shall also not apply to data or information requested in connection with a compliance or enforcement action under Section 215 of the Federal Power Act, Section 400 of these Rules of Procedure, or any procedures adopted pursuant to those authorities, in which case the Rules of Procedure applicable to the production of data or information for compliance and enforcement actions shall apply.*
>
> ***1606. Expedited Procedures for Requesting Time-Sensitive Data or Information***
> *1. In the event NERC or a regional entity must obtain data or information by a date or within a time period that does not permit adherence to the time periods specified in Section 1602, the procedures specified in Section 1606 may be used to obtain the data or information. Without limiting the circumstances in which the procedures in Section 1606 may be used, such circumstances include situations in which it is necessary to obtain the data or information (in order to evaluate a threat to the reliability or security of the bulk-power system, or to comply with a directive in an order issued by the Commission or by another ERO governmental authority) within a shorter time period than possible under*

Section 1602. The procedures specified in Section 1606 may only be used if authorized by the NERC Board of Trustees prior to activation of such procedures.

2. Prior to posting a proposed request for data or information, or a modification to a previously-authorized request, for public comment under Section 1606, NERC shall provide the proposed request or modification, including the information specified in paragraph 1602.2.1 or 1602.2.2 as applicable, to the Commission's Office of Electric Reliability. The submission to the Commission's Office of Electric Reliability shall also include an explanation of why it is necessary to use the expedited procedures of Section 1606 to obtain the data or information. The submission shall be made to the Commission's Office of Electric Reliability as far in advance, up to twenty-one (21) days, of the posting of the proposed request or modification for public comments as is reasonably possible under the circumstances, but in no event less than two (2) days in advance of the public posting of the proposed request or modification.

3. NERC shall post the proposed request for data or information or proposed modification to a previously-authorized request for data or information for a public comment period that is reasonable in duration given the circumstances, but in no event shorter than five (5) days. The proposed request for data or information or proposed modification to a previously-authorized request for data or information shall include the information specified in paragraph 1602.2.1 or 1602.2.2, as applicable, and shall also include an explanation of why it is necessary to use the expedited procedures of Section 1606 to obtain the data or information.

4. The provisions of paragraphs 1602.3, 1602.4. 1602.5 and 1602.6 shall be applicable to a request for data or information or modification to a previously-authorized request for data or information developed and issued pursuant to Section 1606, except that (a) if NERC makes minor changes to an authorized request for data or information without board approval, such changes shall require board approval if a reporting entity objects to NERC in writing to such changes within five (5) days of issuance of the modified request; and (b) authorization of the request for data or information shall be final unless an affected party appeals the authorization of the request by the Board of Trustees to the ERO governmental authority within five (5) days following the decision of the Board of Trustees authorizing the request, which decision shall be promptly posted on NERC's web site.

Bright-Line Determination Survey

Attachment I contains a generic list of those SSCs that could;

- potentially impact the reliable delivery of electricity to the Bulk Power System; but
- *do not impact* safety functions, security functions, and emergency response functions as defined by the NRC's authority under 10 C.F.R. Section 73.

Attachment II contains a generic list of those SSCs that could:

- potentially impact the reliable delivery of electricity to the Bulk Power System; and
- could also *impact* safety functions, security functions, and emergency response functions as defined by the NRC's authority under 10 C.F.R. Section 73.

Attachments I and II are to be used only for purposes of completing the Bright-Line Survey. Compliance to the applicable CIP Reliability Standards will be determined in accordance with the FERC approved implementation plan.[4]

To assist NERC in determining those SSCs that should be exempted from NERC CIP Reliability Standards because they are subject to the NRC's cyber security regulations or other applicable authority (i.e., the "Bright-Line"); please complete the following Survey Question:

Survey Question 1: Does Attachment I, as written, include all SSCs[5] in the balance of plant of your power plant that *could* impact the reliable delivery of electricity to the Bulk Power System, but *do not impact* safety functions, security functions, or emergency response functions as defined in 10 C.F.R. Section 73?[6]

☐ YES

☐ NO

If the answer to this question is "no", please make any corrections to the existing systems list in Attachment I to include all applicable systems. Additionally, please identify those components that should be excluded from the systems identified in Attachment I that would have functions as defined in 10 C.F.R. Section 73. Please include an explanation justifying your changes.

After completing the Survey Items above, please complete the *Organization Information and Approval* section below and return the completed survey as indicated in the *Due Date and NERC Contact Information* section above.

---

[4] The FERC-approved Implementation Plan for NPPs is available at: http://www.nerc.com/files/NERC_706B_Implementation_Plan.pdf.

[5] Attachment I and II are system level reviews. However, there may be a "component(s)" in a system listed in Attachment I that would fall under 10 CFR 73.54. This component(s) should be listed in Attachment I for exclusion to that system by the NPP as it applies.

[6] 10 CFR 73 is available at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/.

Organization Information and Approval

Nuclear Plant System Engineering Contact Information

NPP Name:	NERC Compliance Registry #:
Contact Name:	Contact Title:
Office Phone:	Cell Phone:
Email:	Additional Information:

Approval

To the best of my knowledge, the information provided in the response to this survey is correct.

Supervisor approving this survey:[7]

Name:

Date:

Title:

[7] This approval should be completed by a company employee that is a supervisor-level or above and that has the ability to verify that technically-appropriate individual(s) completed survey item 1.

Attachment I

Generic Identification of Systems, Structures and Components (SSCs) Potentially Subject to NERC CIP Reliability Standards

Attachment I is a system level review. However, NERC recognizes that there may be a plant specific "component(s)" in a system listed in Attachment I that may fall under 10 C.F.R. Section 73.54. This component(s) should be listed in Attachment I for exclusion to that system by the NPP as it applies to your facility.

Water Systems

- Heater/Drain System
- Condensate System
- Water Cleanup System, Chemical Treatment
- Circulating Water
- Non-Safety Cooling Water
- Feedwater Lube Oil System

Steam Systems

- Extraction Steam
- Gland Steam

Generator

- Generator Exciter and Control Systems
- Generator and Support System
- Electro-hydraulic System – (Excluding Fast Acting Solenoid Valve)
- Nitrogen, CO2, and Hydrogen Systems
- Isophase Bus Duct Cooling
- Lube Oil System

Miscellaneous

- Air Removal System (Pressurized Water Reactor)
- Station and Service Air System
- Computer systems and SSCs feeding Energy Management System (EMS)

Power

- Switchyard
- Non-Safety Related Power Distribution (AC/DC)

Comments/basis for changes to Attachment I:

NOTE: Please attach additional documents that complete *Survey Question* 1 if required.

Attachment II

Generic Identification of SSCs Potentially Subject to NRC Cyber Security Regulations

NERC recognizes that the following lists of SSCs are generic in nature and may include some SSCs that could be subject to compliance with NERC CIP Reliability Standards and therefore should be included on Attachment I.

Safety Related Water Systems

- Main Feedwater System
- Condensate system (CSTs for Feedwater supply)
- Ultimate Heat Sink system

Steam Systems

- Main Steam System

Generator

- Generator Control System that feeds into Reactor Protection System (RPS) (Fast Acting Solenoid Valve)

Power

- Safety Related Power Distribution (AC/DC)
- Power systems that feed the RPS (LOOP signal, etc.)

Miscellaneous

- Air Removal System (Boiling Water Reactor)
- Reactor Protection System
- Rod Control System
- Reactor Regulating System
- ATWS Mitigation System Actuation Circuitry (AMSAC)

Qualifying comments on Attachment II, if needed:

ATTACHMENT B

August 27, 2010 NERC Letter to Nuclear Power Plants in Response to Survey

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

August 27, 2010

NERC's Response to the completed Bright Line Survey: [NPP Name]

Contact and address here
[Email]

RE: Receipt of the Completed 706-B Bright-Line Survey

Dear _____:

The North American Electric Reliability Corporation ("NERC") is in receipt of your nuclear power plant's ("NPP") completed NERC 706-B Bright Line Survey. In your survey response you state that the balance of plant ("BOP") systems structures and components ("SSCs") listed in the survey are associated with "important to safety" functions or "support systems and equipment which, if compromised, would adversely impact safety", and therefore are subject to the Nuclear Regulatory Commission's ("NRC") jurisdiction.[1]

NERC is currently consulting with the NRC to determine if these SSCs are within the scope of NRC's jurisdiction. In order for NERC to verify that these BOP SSCs are covered under the NRC's jurisdiction, and therefore not subject to NERC jurisdiction, NERC is requiring that each NPP provide the NRC with a notification letter identifying all BOP SSCs considered important to safety. Additionally, NERC is requiring that each NPP submit a revised cyber security plan to the NRC for its review and approval. If the NRC determines that these BOP SSCs are not within the scope of its jurisdiction, these BOP SSCs will remain subject to compliance with the applicable NERC CIP Reliability Standards as identified in the FERC-approved NPP implementation plan. At such time, NERC may initiate an on-site Spot Check audit within 30 calendar days in accordance with the NERC Compliance Monitoring and Enforcement Program ("CMEP").[2]

NERC is requiring each NPP to submit the notification letter described above to the NRC, with a copy to NERC within thirty (30) calendar days after receipt of this letter.

For your convenience, NERC has developed a webpage providing additional information regarding the 706-B project: http://www.nerc.com/page.php?cid=3|23|347.

[1] The applicable continuity of power systems (BOP) support the reliability of the bulk-power system, but could also directly or indirectly impact reactivity.
[2] The NERC CMEP is available on NERC's website at: http://www.nerc.com/page.php?cid=1|8|169.

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Any questions may be directed to Jim Hughes via email at Jim.Hughes@nerc.net or by telephone at 609.203.2288. In addition to your normal NRC correspondence docketing process, please ensure to include Jim Hughes at:

Cc: Jim Hughes
NERC
116-390 Village Boulevard
Princeton, NJ 08540

Jim T. Wiggins
Director, Office of Nuclear Security & Incident Response
Two White Flint North (MS: 4D22A)
11555 Rockville Pike
Rockville, MD 20852-2738

Eric Leeds
Director, Office of Nuclear Reactor Regulation
One White Flint North (MS: 13H16M)
11555 Rockville Pike
Rockville, MD 20852-2738

Respectfully,

Michael Moon
Director of Compliance Operations

ATTACHMENT C

September 17, 2010 NRC/NERC Security Standards Gap Analysis – White Paper

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NRC/NERC Security Standards Gap Analysis

September 17, 2010

Introduction

Nuclear Power Plant (NPP) Balance Of Plant (BOP) Systems, Structures, and Components (SSC) that are continuity of power systems are considered to be under the North American Electric Reliability Corporation's (NERC) jurisdiction and therefore outside the purview of the Nuclear Regulatory Commission (NRC). However, NERC is to develop an ERO exception process to move any of these SSCs from NERC to the NRC's jurisdiction. NERC, in consultation with the NRC, and oversight from the Federal Energy Regulatory Commission (FERC), are to develop this ERO process that ensures there are no regulatory gaps in accordance with section 50 of FERC Order 706-B and the Memo of Understanding (MOU) executed between the NRC and NERC.[1]

NERC provided each NPP a generic "Bright-line" survey June 2010 to establish a solid jurisdictional boundary between NERC and the NRC, requiring each NPP's input for plant specific exclusions.[2] The NPPs completed and presented their surveys to NERC during July and August of 2010. Subsequent review of the completed surveys indicates that all 104 NPPs are taking the position that the BOP continuity of power systems should be excluded from NERC jurisdiction and moved to the NRC's jurisdiction. The NPP suggest that these BOP systems should be classified under title 10 of the code of federal regulations (10 CFR), specifically §73.54 (a)(1)(i) & (iv). The following is the synopsis regarding the basis for this position:

> "The majority of the systems in Table 1 *(BOP SSCs)* may support the reliability of the bulk-power system, but could also directly or indirectly impact reactivity."…" We have not identified systems in the Balance of Plant that could impact bulk-power reliability that do not also have an impact on reactivity."

Therefore, per FERC Order 706-B and the MOU, it is the intent of this white paper to identify any regulatory gaps, analyze these gaps, and provide proposed actions for management's consideration. The documents assessed for this gap analysis are the NRC Regulatory Guide 5.71 (reference 2), NEI 08-09 (reference 6), NRC rules (references 1-5 & 7) as they apply, and the NERC CIP Reliability Standards (reference 8). These references are subject to change and thus this gap analysis may require subsequent revisions as well.

[1] Applicable 706-B Bright-Line project documents may be found at: http://www.nerc.com/page.php?cid=3|23|347.
[2] NERC, in coordination with the NRC, developed a generic list of BOP continuity of power SSCs.

Approach and Executive Summary

NERC, in coordination with and contribution from the NRC, and with consideration of information provided by Nuclear Energy Institute (NEI), has determined that the controls identified in the NRC rules are equal to or better than the NERC CIP Standards. However, minor differences are identified below, in Attachment I, and the *Gap Analysis* section of this report. It is the consensus of the team that these differences, with the recommended proposed action, would not negatively impact the reliability of the Bulk Electric System (BES) if the NRC controls were implemented on the applicable BOP systems. However, there is one possible gap identified in the regulatory guide that should be addressed:

1. The present language in the NRC rules, specifically Regulatory Guide 5.7,1 may allow the NPP to remove from scope those BOP systems that could be in scope under the NRC physical and cyber rules for "Critical Systems". The applicable language in section C.3.1.3 of the Regulatory Guide states, in part, "…a compromise of these plant systems could result in radiological sabotage (i.e., significant core damage) and therefore has the potential to adversely impact the public health and safety. Although all of these systems may not ultimately be within the scope of the licensee's cyber security program, the licensee's accurate identification of these plant systems associated with a SSEP function is essential to the development of an effective cyber security program…"[3] If these BOP systems are classified under 10 CFR §73.54 (a)(1)(i) & (iv), because they could impact reactivity, the NPP may also take the position that these systems do not have the capability to cause "significant core damage" and therefore not required to be "Critical Systems" as identified in the Regulatory Guide 5.71 or NEI 08-09.[4] This creates a potential vulnerability that makes it possible for the continuity of power BOP systems to avoid compliance with the NRC physical and cyber security rules. Refer to the Proposed Actions section below for recommendations to address this possible gap.

Proposed Actions

In order to address the potential regulatory gap identified above, it is recommended that the NERC survey response letter to the NPPs require that each NPP initiate a notification letter to the NRC that states the applicable BOP continuity of power systems would be classified under 10 CFR §73.54 (a)(1)(i) & (iv) and therefore implement the applicable NRC physical and cyber security controls. Additionally, inform the NPP that NERC, in consultation with the NRC, will review the NPP's site specific "Critical Systems" and "Critical Digital Assets" lists to verify that the continuity of power systems are in scope under the NRC's physical and cyber security controls. It is understood that until the NRC makes its final policy decision regarding the NPP's letter, these BOP SSCs remain under NERC's jurisdiction.

[3] Safety, security, and emergency preparedness (SSEP) functions as identified in 10 CFR 73: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html.
[4] NRC Regulatory Guide may be found on the NRC's website at: http://nrc-stp.ornl.gov/slo/regguide571.pdf.

Gap Analysis – Less Gap Identified in Executive Summary

After thorough review of the information in Attachment I, the following are the areas where apparent gaps were identified between the NERC CIP Standards and the various NRC controls (NEI 08-09, Regulatory Guide 5.71, and NRC CFR) were identified with subsequent impact assessment provided for each:

Asset Identification: In scope cyber assets are called Critical Cyber Assets or CCAs under NERC's CIP Standards. NEI 08-09 and Regulatory Guide 5.71 call in scope assets first "Critical Cyber Systems" and the components in the systems are called "Critical Digital Assets" or CDAs. This is simply a naming issue and therefore, the controls that the NRC have in place are equal to or better than the controls established in the NERC CIP controls.

Access Authorization: NERC requires a criminal background check to go back seven (7) years. However, NRC rules require five (5) years. While the NRC control seems to be less stringent than the NERC control, there are additional NRC controls that require criminal background checks to be re-performed every five (5) years per 10 CFR 73.56.[5] The NRC controls require that criminal and financial background be re-performed every three (3) years for critical positions. The NRC also requires every manager and supervisor to be annually trained on the Continuous Behavioral Observation Program (CBOP) to identify and act on employees that exhibit "aberrant" behavior. Therefore, the controls that the NRC has in place are equal to or better than the controls established in the NERC CIP controls.

Physical Security (6 wall): NERC requires a six wall control for CCAs where the NRC controls explicitly do not. However, the NRC controls established in 10 CFR §73 "Design Basis Threat" are equal to or better than the controls established in the NERC CIP controls. [6]

Identification of Sr. Manager/ Delegate: NERC requires the entity to identify the facility's Sr. manager and delegate. While this is not specifically identified in NEI 08-09 or Regulatory Guide 5.71, these controls do require the identification of a "cyber security team". Each NPP is to follow the controls established in 10 CFR §50 Appendix B for a quality assurance program regarding procedures, configuration management (engineering and configuration changes), and document management (new procedure/ revision control).[7] Additionally, each NPP is required to identify key management personnel per their docketing and licensing process. Therefore, the NRC controls are equal to or better than the controls established in the NERC CIP controls.

Changes and Exceptions to the Security Policy/System(s): The NERC CIP standards provide detailed requirements on documenting changes in this area whereas NEI 08-09 and Regulatory Guide 5.71 do provide some controls in this area. However, the NRC requires additional and more stringent controls established in 10 CFR §50.59 "Changes,

[5] 10 CFR 73.56 can be found on the web at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html#part073-0056.
[6] 10 CFR 73 is found on the web at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html#part073-0001.
[7] 10 CFR 50 Appendix B can be found on the web at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html.

tests and experiments"[8] for physical changes to the facility as described in the NPP's Safety Analysis Report. This requires each NPP to analyze the proposed change and to have NRC's approval prior to implement any changes to the Security plan or SSCs in scope under 10 CFR §73.54 (a)(1)(i) & (iv) if the proposed changes are less than the present design/procedure. Additional controls are established in 10 CFR §50 Appendix B (Engineering, Procurement, Procedures, & Document Control) and the licensing basis established by the licensee within their security plan. Therefore, the NRC controls are equal to or better than the controls established in the NERC CIP controls.

Periodicity of implementing changes: NERC requires various periodicities of certain activities such as the time for employee revocation of physical and logical access to the entity's ESP for cause, reassigned, or quits, and procedure changes. While there are no controls established for this specifically in NEI 08-09 or Regulatory Guide 5.71, the NRC controls require notification to the NRC for cause and each NPP is required to establish an out processing procedure that is maintained under 10 CFR 50 Appendix B. This process clearly identifies the NPP's responsibilities for employees that are let go for cause where security escorts the individual off-site and badge rights and logical access are immediately revoked. When an employee quits or is reassigned away from the NPP, there is a management check off sheet where the employee must complete a sign off for each applicable area the employee no longer is required to have physical or logical access to. Therefore, the NRC controls are equal to or better than the controls established in the NERC CIP controls.

Event Analysis and Corrective Actions: NERC requires various reporting of security and cyber deficiencies/ events and subsequent corrective actions documented. While NEI 08-09 and Regulatory Guide 5.71 do provide similar controls in this area, the NRC controls addressing the corrective action program are provided in 10 CFR §50 Appendix B in the "Corrective Action" criteria. Additionally, the nuclear industry's Corrective Action, apparent and root cause programs are mature, well defined, and well inspected by the NRC and the Institute of Nuclear Power Operations (INPO).[9] Therefore, the NRC controls are equal to or better than the controls established in the NERC CIP controls.

Control of Critical Energy Infrastructure Information (CEII): NERC requires various controls surrounding the identification, management, and protection of CEII. While NEI 08-09 and Regulatory Guide 5.71 do provide equivalent controls, the NRC provides more stringent controls surrounding "Safe Guards Information" (SGI) as identified in 10 CFR §73.21 and §73.22.[10] These controls require special training, "need to know", FBI clearances, and SGI security cabinets with special locks. SGI is required to have proper stamping to help protect against unauthorized disclosure. Additionally, the individual who discloses SGI without NRC authorization is subject to criminal and civil charges under the NRC rules. Therefore, the NRC controls are equal to or better than the controls established in the NERC CIP controls.

[8] 10 CFR 50.59 is found on the web at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0059.html.
[9] INPO's website: http://www.inpo.info/. With additional information on HSS: http://www.hss.energy.gov/csa/csp/inpo/.
[10] 10 CFR 73.21 is found on the web at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html#part073-0021.

Remedial Action Directives (RAD): NERC may issue remedial actions and directives to a bulk power system owner, operator, or user to resolve an alleged violation of a reliability standard by addressing conditions, practices, or any other relevant action or activity (Per section 6 of Reference 9). The NRC has similar rules as identified in 10 CFR Part 2 Subpart B "Procedure for Imposing Requirements by Order, or for Modification, Suspension, or Revocation of a License, or for Imposing Civil Penalties".[11] This rule allows the NRC to issue orders up to and including revocation of the license to operate the NPP. Additionally, the NRC issues the NPPs "Information Notices" to provide significant recently identified information about safety, safeguards, or environmental issues. NPPs are expected to review the information for applicability to their facilities and consider appropriate actions to avoid similar problems.[12] Therefore, the NRC controls are equal to or better than the controls established in the NERC CIP controls.

Regulatory Guide 5.71 and NEI 08-09: The NRC's rules are performance based rules. As such, each NPP is required to review the rule and submit to the NRC, via a docketing process, how they will meet the rule. Once the NPP's submittal is approved by the NRC, this becomes the licensing basis for that NPP and enforceable by the NRC. Regarding Regulatory Guide 5.71 and NEI 08-09, these are guidelines that are acceptable by the NRC for each NPP to use to be in compliance with 10 CFR §73 via the licensing process. Once these are submitted to the NRC with NPP specific information, subsequently approved by the NRC, this now becomes part of the NPP's licensing basis and enforceable by the NRC. Therefore, the NRC controls are equal to or better than the controls established in the NERC CIP controls.

References

1. 10 CFR §73 "Physical Protection of Plants and Materials"
2. Regulatory Guide 5.71 "Cyber Security Programs for Nuclear Facilities"
3. 10 CFR §50.59 "Changes, tests and experiments"
4. 10 CFR §50 Appendix B "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
5. 10 CFR §50 Appendix A "General Design Criteria for Nuclear Power Plants"
6. NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors"
7. 10 CFR Part 2 Subpart B "Procedure for Imposing Requirements by Order, or for Modification, Suspension, or Revocation of a License, or for Imposing Civil Penalties"
8. NERC CIP Standards CIP-002 through CIP-009[13]
9. NERC Rules of Procedure Appendix 4B "Sanction Guidelines of the North American Electric Reliability Corporation"

[11] 10 CFR Part 2 is found on the web at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part002/.
[12] NRC "Information Notices" may be found at: http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/.
[13] NERC CIP standards are found on the web at: http://www.nerc.com/page.php?cid=2|20.

.

Table of Contents

BES Cyber System Categorization

CIP 002-4 Requirement[14]	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R1	10 CFR 73.54(a)(1)	C.3.1.3 Identification of Critical Digital Assets	Yes-	10 CFR 73.54 (a)(1) 10 CFR 73.54 (b)(1) A.3.1.3	Yes- Step 1 – Identify critical systems, Step 2, Identify critical digital assets
R1.1	Same language	C.3.3.2.9 Configuration Management	Yes-	10 CFR 73.54 (d)(2) 10 CFR 73.54 (d)(3) A.4.4.1 A.4.4.2 A.4.5 E.4	Yes- Covered in 50.59 and Appendix B (of Part 50).
R1.2	10 CFR 73.54(a)(1)	C.3.1.3 Identification of Critical Digital Assets	Yes-	10 CFR 73.54 (h) A.4.13	Yes- Covered in 50.59 and Appendix B (of Part 50).
R2	Same language applies, just in scope	C.3.3.2.9 Configuration Management	Yes- Also covered under 10 CFR 50.59	10 CFR 73.54 (h) A.4.13	For NPPs – Critical systems are identified, and change management.
R2.1	10 CFR 73.54(a)(1)	C.3.1.3 Identification of Critical Digital Assets	Yes-	10 CFR 73.54 (h) A.4.13	Yes-
R2.2	Docketing and licensing process addresses this requirement.		Docketing and licensing process addresses this requirement.	All are owned by Plant	Yes-
R2.3	10 CFR 73.54(a)(1)	C.3.1.3 Identification of Critical Digital Assets	Yes- Based on the criteria for determining what is a CDA as outlined in RG 5.71	50.59 processes. Impact done in A.4.4.2 and A.4.5	Yes-

[14] Used the draft version of V4 (December 2009)

CIP 002-4 Requirement[14]	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
			(i.e., a compromise could lead to significant core damage) the impact categorization is always the same – HIGH.		
R3	10 CFR 73.54(e)(2) and (f)	C.3.1.3 Identification of Critical Digital Assets	Yes-	See below.	Yes-
R3.1	10 CFR 73.54(a)(1)	C.3.1.3 Identification of Critical Digital Assets	Yes-	A.3.1.3 Also 10 CFR 50.65, Maintenance Rule And configuration management program.	Yes- Also 10 CFR 50.65, Maintenance Rule And configuration management program.
R3.2	10 CFR 73.54(a)(1)	C.3.1.3 Identification of Critical Digital Assets	Yes- Furthermore, based on the criteria for determining what is a CDA as outlined in RG 5.71 (i.e., a compromise could lead to significant core damage) the impact categorization is always the same – HIGH.	A.3.1.3	Yes- All systems protected by the cyber security program are critical, and are protected with high assurance.

Security Management Controls

CIP 003-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R1	10 CFR 73.54(f)	A.1	Yes-	Cyber Security Plan	Yes-
R1.1	10 CFR 73.54(f)	A.2.1	Yes-	Cyber Security Plan	Yes-
R1.2	10 CFR (d)(2) Requires training and awareness for all personnel	C.3.3.2.8 Awareness and Training	Yes-	The Plan Template is publicly available. Users are trained in A.4.8 10 CFR 50 Appendix B	Additionally, in Training (A.4.8) and Documentation Control
R1.3	10 CFR 73.55(m) Review program every 24 months, within 12 months if change is significant	A.3.1.1 Security Assessment and Authorization	Yes-	10 CFR Appendix B 10 CFR 73.54 (g) A.4.12 - The CSP is reviewed in accordance with 10 CFR 73.55 (m) which requires a review at a minimum every 24 months.	Yes-
R2	08-09 and 5.71 require this to be documented 10 CFR 50 Appendix B	C.3.1.2 Define Roles and Responsibilities and Form the Cyber Security Team	Yes-	A.4.11 Appendix B SAR as updated	Yes-

CIP 003-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R2.1	08-09 and 5.71 require this to be documented 10 CFR 50 Appendix B	C.3.1.2 Define Roles and Responsibilities and Form the Cyber Security Team	Yes- In addition 10 CFR 50 Appendix A applies	Appendix B	Yes-- Not in guide, but covered elsewhere.
R2.2	10 CFR 50 Appendix B 10 CFR 73.55(m)		Managed through the NPP Configuration Management Process	Appendix B	Yes-- Not in guide, but covered elsewhere.
R2.3	Managed through the NPP Configuration Management Process	Managed through the NPP Configuration Management Process	Managed through the NPP Configuration Management Process	Appendix B	Yes-- Not in guide, but covered elsewhere.
R2.4	10 CFR 50 Appendix B	C.3.1.2 Define Roles and Responsibilities and Form the Cyber Security Team	Yes-	Any deviations from the CSP that could decrease the effectiveness of the plan must be reviewed by the NRC in accordance with 10 CFR 50.90 Appendix B	Yes-- Not in guide, but covered elsewhere.

CIP 003-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R3	10 CFR 74.54 (a) – High Assurance of Adequate Protection against cyber attacks up to and including the DBT 10 CFR 73.54(c)(1) – Implement security controls License Condition: 10 CFR 50 – 3 step process of addressing controls is a license condition	C.3.3 Security Controls	Yes-	Any deviations from the CSP that could decrease the effectiveness of the plan must be reviewed by the NRC in accordance with 10 CFR 50.59 Appendix B	Yes-- Not in guide, but covered elsewhere.

CIP 003-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R3.1	10 CFR 50.59 – changes that reduce effectiveness have to be approve by the NRC before the change can be implemented 10 CFR 73.54 (f) – Must maintain policies and procedures	C.3.3 Security Controls	Yes-	50.59 - Exceptions must be approved in advance by the NRC if the change could result in a decrease in effectiveness. A.3.1.6 - With specific controls, alternate controls, or not applying a control must show that the alternate is equivalent or better, or that there is no attack vector.	Yes-
R3.2	10 CFR 50.59 – changes that reduce effectiveness have to be approve by the NRC before the change can be implemented 10 CFR 73.54 (f) – Must maintain policies and procedures	C.3.3 Security Controls	Yes-	Any deviations from the CSP that could decrease the effectiveness of the plan must be reviewed by the NRC in accordance with 10 CFR 50.59 Also A.3.1.6	Yes-

CIP 003-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R3.3	10 CFR 50.59 – changes that reduce effectiveness have to be approve by the NRC before the change can be implemented 10 CFR 73.54 (f) – Must maintain policies and procedures	C.3.3 Security Controls	Yes-	Licensing actions are submitted under oath or affirmation. Reviews as required by 73.54(g) and 50.59	Yes-
R4	10 CFR 73.21 – 10 CFR 73.22 10 CFR 73.57 10 CFR 73.54 (c)	A. Introduction B.3.7 Transmission Confidentiality B.3.20 C.3.1 System and Information Integrity Policy and Procedures	Yes-	10 CFR 73.21, "Protection of Safeguards Information" QA Records Program under 10 CFR 50 Appendix B. A.4.13, D.2.9	Yes-
R4.1	10 CFR 73.21 10 CFR 73.22 10 CFR 73.57 10 CFR 73.54 (c)	Covered by other regulations (SGI, SUNSI, 10 CFR 2.390)	Covered by other regulations (SGI, SUNSI, 10 CFR 2.390)	See above. A.4.13 These are QA records and may not be safeguards.	Yes-

CIP 003-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R4.2	10 CFR 73.21 10 CFR 73.22 10 CFR 73.57 10 CFR 73.54 (c)	Covered by other regulations (SGI, SUNSI, 10 CFR 2.390)	Covered by other regulations (SGI, SUNSI, 10 CFR 2.390)	See above. 10 CFR 73.21 and QA Records	Yes-
R4.3	10 CFR 73.21 - For control of SGI, there is no time period in the rule, this is a continuous requirement – 73.55(m) requires 24 month full review of entire program 10 CFR 73.22 10 CFR 73.57 10 CFR 73.54 (c)	Covered by other regulations (SGI, SUNSI, 10 CFR 2.390)	Covered by other regulations (SGI, SUNSI, 10 CFR 2.390)	10 CFR 73.54 (g) A.4.12 Appendix B (Corrective Action Program)	Yes-
R5	10 CFR 73.21 10 CFR 73.22 10 CFR 73.56 – Critical Group and Access authorization programs	Already addressed in the physical security programs	Already addressed in the physical security programs	10 CFR 73.21 and QA Records program	Yes-

CIP 003-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R5.1	10 CFR 73.21 10 CFR 73.22 10 CFR 73.56 – Critical Group and Access authorization programs	Already addressed in the physical security programs	Already addressed in the physical security programs	10 CFR 73.21 and QA Records program	Yes-
R5.1.1	10 CFR 73.21 10 CFR 73.22 10 CFR 73.56 – Critical Group and Access authorization programs	Already addressed in the physical security programs	Already addressed in the physical security programs	10 CFR 73.21 and QA Records program	Yes-
R5.1.2	10 CFR 73.21 10 CFR 73.22 10 CFR 73.56 – Critical Group and Access authorization programs	Already addressed in the physical security programs	Already addressed in the physical security programs	10 CFR 73.21 and 10 CFR 73.54 (g)	Yes-

CIP 003-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R5.2	10 CFR 73.21 10 CFR 73.22 10 CFR 73.56 – Critical Group and Access authorization programs Requalify	Already addressed in the physical security programs	Already addressed in the physical security programs	10 CFR 73.21 10 CFR 73.55 (m)	Yes-
R5.3	10 CFR 73.21 10 CFR 73.22 10 CFR 73.56 – Critical Group and Access authorization programs	Already addressed in the physical security programs	Already addressed in the physical security programs	10 CFR 73.21 10 CFR 73.55 (m)	Yes-
R6	10 CFR 73.54 (d)(3) 10 CFR 50.59	C.3.3.2.9 Configuration Management	Yes-	10 CFR 50 10 CFR 73.54 (d)(3) Appendix B A.4.4.1 A.4.4.2 A.4.5 E.4, E.10	Yes-

Personnel and Training

CIP 004-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R1	10 CFR 73.54(d)(1)	C.3.1.2 Define Roles and Responsibilities and Form the Cyber Security Team: C.10.2 Awareness Training	Yes-	10 CFR 73.54 (d)(1) A.4.8 E.9	Yes-
R2	10 CFR 73.54(d)(1)	C.10.3 Technical Training C.10.4 Specialized Cyber Security Training	Yes-	10 CFR 73.54 (d)(1) A.4.8 E.9 (E.9.2 and E.9.3)	Yes-
R2.1	10 CFR 73.54(d)(1)	C.3.3.2.8 Awareness and Training	Yes-	10 CFR 73.54 (d)(1) A.4.8 E.9 (E.9.3), (E.9.4)	Yes-
R2.2	10 CFR 73.54(d)(1) 10 CFR 73.54(b)(3) 10 CRR 73.55(a)(1)	A.2.2 Performance-Based Requirements	Yes-	10 CFR 73.54 (d)(1) A.4.8 E.9	*Yes*-
R2.2.1	10 CFR 73.54(d)(1) 10 CFR 73.54(b)(3) 10 CRR 73.55(a)(1)	A.2.2 Performance-Based Requirements	Yes-	Requirements in this area reside outside the Cyber Security Plan. Cyber security aspects are covered in E.9	Yes-
R2.2.2	10 CFR 73.54(d)(1) 10 CFR 73.54(b)(3) 10 CRR 73.55(a)(1)	A.2.2 Performance-Based Requirements	Yes-	A.4.8 E.9.2	Yes-

CIP 004-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R2.2.3	10 CFR 73.54(d)(1) 10 CFR 73.54(b)(3) 10 CRR 73.55(a)(1)	A.2.2 Performance-Based Requirements	Yes-	A.4.8 E.9.2	Yes-
R2.2.4	10 CFR 73.54 (e)(2) 10 CFR 73.54(d)(1)	C.8.2 Incident Response Training C.8.3 Incident Response Testing and Drills C.8.4 Incident Handling C.9.4 Contingency Plan Training	Yes-	A.4.8 and A.4.11 E.7.2 E.8.3 E.9.2, E.9.3, E.9.4	Yes-
R2.3	10 CFR 73.54(d)(1)	C.8.2, C.8.3, C.8.4 and C.9.4 C.10.8 Security Training Records	Yes-	Period is not specified for general awareness training. For others, annually.	Yes-
R3	10 CFR 73.56 – Access Authorization 10 CFR 73.57 – Criminal record checks	C.3.3.2.2 Personnel Security	Yes-	10 CFR 73.55, 10 CFR 73.56, 10 CFR 73.57 PSP, RG 5.77 NEI 08-09, Revision 6, D.1, E.2, E.5	Yes-

CIP 004-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R3.1	10 CFR 73.56 – Access Authorization 10 CFR 73.57 – Criminal record checks	C.2.1 Personnel Security Policy and Procedures C.2.2 Personnel Termination or Transfer	Yes-	FBI assessment is a 5 year check.	Gap – we do 5 years rather than 7. But we have an ongoing Behavioral Observation Program.
R3.2	10 CFR 73.56 – Access Authorization 10 CFR 73.57 – Criminal record checks	C.2.1 Personnel Security Policy and Procedures C.2.2 Personnel Termination or Transfer	Yes- Specific requirements provided in Title 10 of the Code of Federal Regulations (10 CFR) 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants."	73.56 (h)(1)(v)(A) and (B) - (check) (A) A criminal history update and credit history re-evaluation for any individual with unescorted access. The criminal history update and credit history re-evaluation must be completed within 5 years of the date on which these elements were last completed.	Yes-

CIP 004-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R3.3	10 CFR 73.56 – Access Authorization 10 CFR 73.57 – Criminal record checks	C.2.1 Personnel Security Policy and Procedures C.2.2 Personnel Termination or Transfer	Yes- Specific requirements provided in Title 10 of the Code of Federal Regulations (10 CFR) 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants."	10 CFR 73.56 For denial (m)(2) (m)(4) Audited (n) Records (o) NEI 08-09: D.1, E.2	Yes-
R4	10 CFR 73.56 – Access Authorization 10 CFR 73.57 – Criminal record checks	B.1.1 Access Control Policy and Procedures	Yes-	10 CFR 73.55, 10 CFR 73.56, 10 CFR 73.57 PSP, RG 5.77 NEI 08-09, R6, D.1, E.2, E.5	Yes-
R4.1	10 CFR 73.54 (d) (1)	B.1.2 Account Management	Yes-	D.1.1 D.1.2 E.2	Yes-

CIP 004-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R4.2	10 CFR 73.56 – individual must be deemed trustworthy to have unauthorized access, if an individual is deems to be untrustworthy access must be revoked immediately. 10 CFR 73.56 – requires electronic system that entire industry uses and shares information	B.1.2 Account Management	Yes-	D.1.1 – Links to Access Authorization Program D.1.2 E.2 (“upon termination” or, at most, every 31d) NEI 03-01, “Nuclear Power Plant Access Authorization Program,” states “On the day of termination”	Yes-

Electronic Security Perimeter

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R1	10 CFR 73.54 (c)(2) – Maintain defense in depth to prevent, detect and recovery from attacks	C.3.2 Defense-in-Depth Protective Strategies C.3.2.1 Security Defensive Architecture	Yes-	10 CFR 73.55 10 CFR 73.54 (c)(2) A.3.1.3-6 A.4.3 E.6	Yes-
R1.1	10 CFR 73.54(a)(1) 10 CFR 73.54(c)(2)	C.1 General Requirements C.3.1.4 Review and Validation	Yes-	IBID	Yes-
R1.2	10 CFR 73.54(a) – high assurance of adequate protection	C.3.1.4 Review and Validation Appendix B.3 Critical Digital Asset and Communications Protection	Yes-	No special treatment for Dial Up. See A.4.3 and E.6	Yes-
R1.3	10 CFR 50 appendix B 10 CFR 73.54 (f)	C.3.1.4 Review and Validation Appendix B.3 Critical Digital Asset and Communications Protection	Yes-	A.4.3 and E.6	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R1.4	10 CFR 73.54(a)(1) - high assurance of adequate protection 10 CFR 73.54(c)(2)	C.3.1.4 Review and Validation Appendix B.3 Critical Digital Asset and Communications Protection	Yes-	A.4.3 and E.6	Yes-
R1.5	10 CFR 73.54(a)(1) 10 CFR 73.54(c)(2)	C.3.3 Security Controls	Yes-	A.4.3 and E.6	Yes-
R1.6	10 CFR 50 appendix B 10 CFR 73.54 (f)	C.3.1.2 Define Roles and Responsibilities and Form the Cyber Security Team C.3.1.4 Review and Validation	Yes-	See R1.5 and A.3.1, A.4.4.1, A.4.4.2, A.4.5, Various controls in Appendix D and E	Yes-
R2	10 CFR 73.54 (f) – implement written policies and procedures 10 CFR 73.54 (c) security controls and defense in depth 10 CFR 73.56	Appendix B.1.1 Access Control Policy and Procedures	Yes-	See R1.5, and D.1, D.3, D.5, E.6	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R2.1	10 CFR 73.54 (f) – implement written policies and procedures 10 CFR 73.54 (c) security controls and defense in depth 10 CFR 73.56 10 CFR 73.54(a)(1)(iv)	C.3.3.1.5 System Hardening Appendix B. System Hardening	Yes-	See R1.5 and E.10.8	Yes-
R2.2	10 CFR 73.54 (a) – high assurance of adequate protection (c) – Security Program must provide defense in depth and security controls to accomplish (a) License Condition – 50.59 -	Appendix B.5 System Hardening Appendix B.5.1 Removal of Unnecessary Services and Programs	Yes-	See R1.5 and E.10.8	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R2.3	10 CFR 73.54 (a) – high assurance of adequate protection (c) – Security Program must provide defense in depth and security controls to accomplish (a) License Condition – 50.59 -	C.1 General Requirements C.3.1.3 Identification of Critical Digital Assets C.3.1.4 Review and Validation	Yes-	No special treatment of Dial-Up – all connections secure. See R1.5	Yes-
R2.4	10 CFR 73.54 (a) – high assurance of adequate protection (c) – Security Program must provide defense in depth and security controls to accomplish (a) License Condition – 50.59 -	B.1.4 Information Flow Enforcement	Yes-	See R1.5	Yes-
R2.5		N/A	N/A	A.4.3, A.4.4 and D.1, D.4	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R2.5.1	10 CFR 73.54 (a) – high assurance of adequate protection (f) – requires written policies and procedures to implement program License Condition – 50.59 -	B.1.1 Access Control Policy and Procedures	Yes-	D.1, D.4	Yes-
R2.5.2	10 CFR 73.54 (a) – high assurance of adequate protection (f) – requires written policies and procedures to implement program License Condition – 50.59 -	Appendix B.3.16 Secure Name/Address Resolution Service (Recursive or Caching Resolver) Appendix B.4.1 Identification and Authentication Policies and Procedures Appendix B.4.2 User Identification and Authentication	Yes-	D.1, D.4	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R2.5.3	10 CFR 73.54 (a) – high assurance of adequate protection (f) – requires written policies and procedures to implement program 73.55(m) – review program every 24 months, within 12 if there is a significant change 73.55 – review access within 31 days 73.56 – access authorization program 73.57 – criminal record checks License Condition – 50.59 -	Appendix B.1.1	Yes-	10 CFR 73.54 (g) A.4.4	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R2.5.4	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth License Condition – 50.59 -	Appendix B.3 Critical Digital Asset and Communications Protection	Yes-	E.6	Yes-
R2.6	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth License Condition – 50.59 -	Appendix B.1.1 Access Control Policies and Procedures Appendix B.1.8 System Use Notification	Yes-	D.1.9	Yes-
R3	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth License Condition – 50.59 -	C.5 Records Retention and Handling	Yes-	A.4.4, D.2, E.6	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R3.1	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth (h) record retention License Condition – 50.59 -	Appendix B.3 Critical Digital Asset and Communications Protection	Yes-	See R3	Yes-
R3.2	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth License Condition – 50.59 – they are required to do this in their plan so it becomes a license plan	Appendix B.5.2 Host Intrusion Detection System Appendix C.3.4 Monitoring Tools and Techniques	Yes-	See R3	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R4	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth (e)(2)(iii) – requires licensees to correct exploited vulnerabilities License Condition – 50.59 – vulnerability scans occur quarterly per their plans	Appendix A.4.1.3 Vulnerability Assessments and Scans	Yes-	A.4.4.3.2, E.12	Yes-
R4.1	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth (e)(2)(iii) – requires licensees to correct exploited vulnerabilities License Condition – 50.59 – vulnerability scans occur quarterly per their plans	C.3.2 Flaw Remediation	Yes-	E.12	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R4.2	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth (e)(2)(iii) – requires licensees to correct exploited vulnerabilities License Condition – 50.59 – vulnerability scans occur quarterly per their plans	Appendix A.4.1.3 Vulnerability Assessments and Scans	Yes-	A.4.4.3	Yes-
R4.3	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth (d)(3) – change control (e)(2)(iii) – requires licensees to correct exploited vulnerabilities License Condition – 50.59 – vulnerability scans occur quarterly per their plans	Appendix A.4.1.3 Vulnerability Assessments and Scans	Yes-	A.4.4	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R4.4	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth (d)(3) – change control (e)(2)(iii) – requires licensees to correct exploited vulnerabilities License Condition – 50.59 – vulnerability scans occur quarterly per their plans	Appendix B.1.2 Account Management Appendix B.4.3 Password Requirements	Yes-	A.4.4	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R4.5	10 CFR 73.54 (a) – high assurance of adequate protection (d)(3) – change control (e)(2)(iii) – requires licensees to correct exploited vulnerabilities License Condition – 50.59 – vulnerability scans occur quarterly per their plans Corrective Action Program	Appendix C.3.1.1 Security Assessment and Authorization	Yes-	A.4.4.3.1	Yes-
R5	10 CFR 73.54 (a) – high assurance of adequate protection (d)(3) – change control (f) – written policies and procedures Correction Action Program License Condition – 50.59	C.4.2 Change Control C.4.2.1 Configuration Management C.5 Records Retention and Handling	Yes-	10 CFR 73.54(g) A.4.12 Various other locations.	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R5.1	73.55(m) – everything is reviewed no less often than every 24 months	C.3.3.2.9 Configuration Management	Yes-	10 CFR 73.54(g) A.3.1.5 A.4.4 A.4.12	Yes-
R5.2	10 CFR 73.54 (a) – high assurance of adequate protection (d)(3) – change control (f) – written policies and procedures Correction Action Program License Condition – 50.59 10 CFR 50 appendix B 10 CFR 50 appendix A 10 CFR 50.54(f)	Appendix C.12.5 Developer Security Testing Appendix C.12.6 Applicant testing C.4.2 Change Control	Yes-	Ongoing as part of the change management process via A.3.1.5	Yes-

CIP 005-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R5.3	10 CFR 73.54 (a) – high assurance of adequate protection (c) Defense in depth License Condition – 50.59 – they are required to do this in their plan so it becomes a license plan	C.5 Records retention and Handling	Yes-	10 CFR 73.54(h) A.4.13	Yes-

Physical Security of Cyber Assets

CIP 006-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R1	10 CFR 73.55 – physical security rule 10 CFR 73.54 (b) (3) – incorporate cyber into physical security program	C.3.4 Incorporating the Cyber Security Program into the Physical Protection Program	Yes- The Licensee is required to incorporate their cyber security program into the existing physical security program (10 CFR 73.55) as stated in 10 CFR 73.54(b)(3).	10 CFR 73.54, 73.55, 73.56	Yes-
R1.1	10 CFR 73.55 – physical security rule	C.3.1.4 Review and Validation	Yes-	See R1	Yes-

CIP 006-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	10 CFR 73.54 (b) (3) – incorporate cyber into physical security program License Condition – 50.59 – they are required to do this in their plan so it becomes a license plan				
R1.2	10 CFR 73.55 – physical security rule 10 CFR 73.54 (b) (3) – incorporate cyber into physical security program License Condition – 50.59 – they are required to do this in their plan so it becomes a license plan	C.3.1.4 Review and Validation. Additional controls as required in NRC Rules.	Yes- Part of the existing physical security (protective) plan.	See R1	Yes-
R1.3	10 CFR 73.55 – physical security rule 10 CFR 73.54 (b) (3)	10 CFR 73.55 – physical security rule 10 CFR 73.54 (b) (3) –	Yes- Part of the existing physical security (protective)	See R1	Yes-

CIP 006-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	– incorporate cyber into physical security program License Condition – 50.59 – they are required to do this in their plan so it becomes a license plan.	incorporate cyber into physical security program License Condition – 50.59 – they are required to do this in their plan so it becomes a license plan.	plan.		
R1.4	10 CFR 73.55 – physical security rule 10 CFR 73.54 (b) (3) – incorporate cyber into physical security program 10 CFR 73.56 – access authorization program License Condition – 50.59 – they are required to do this in their plan so it becomes a license plan	See R1.3	Yes- Part of the existing physical security (protective) plan.	See R1	Yes-
R1.5	10 CFR 73.56 – access authorization	See R1.3	Yes- Part of the existing physical	See R1	Yes-

CIP 006-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	rule		security (protective) plan.		
R1.6	10 CFR 73.56 – access authorization rule 10 CFR 73.55 – physical access program	See R1.3	Yes- Part of the existing physical security (protective) plan.	See R1	Yes-
R1.6.1	10 CFR 73.56 (i) – access authorization rule with regard to visitors 10 CFR 73.55 – physical access program.	See R1.3	Yes- Part of the existing physical security (protective) plan.	See R1	Yes-
R1.6.2	10 CFR 73.56 (i) – access authorization rule with regard to visitors 10 CFR 73.55 – physical access program.	See R1.3	Yes- Part of the existing physical security (protective) plan.	See R1	Yes-
R1.7	10 CFR 50.59 – changes must be approved before the change is made 10 CFR 73.55(m) –	10 CFR 50.59 – changes must be approved before the change is made 10 CFR 73.55(m) – review entire program	Yes- Part of the existing physical security (protective) plan.	10 CFR 50.59	Yes-

CIP 006-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	review entire program within 12 months of implementation, then no less often than every 24 months, and within 12 months of changes to personnel, equipment, etc., within 12 months.	within 12 months of implementation, then no less often than every 24 months, and within 12 months of changes to personnel, equipment, etc., within 12 months.			
R1.8	10 CFR 73.55(m) – review entire program within 12 months of implementation, then no less often than every 24 months, and within 12 months of changes to personnel, equipment, etc., within 12 months	See R1.7	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.55(m) requires biannual.	Yes-
R2	10 CFR 73.55 – physical security rule.	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.55 10 CFR 73.54 E.5	Yes-
R2.1	10 CFR 73.55 – physical security rule	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective)	10 CFR 73.55 10 CFR 73.54 E.5	Yes-

CIP 006-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
			plan.		
R2.2	10 CFR 73.55 – physical security rule	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.54 and 55 10 CFR 73.54 E.5	Yes-
R3	10 CFR 73.55 – physical security rule	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.54 and 55 10 CFR 73.54 E.5	Yes-
R4	10 CFR 73.55 – physical security rule	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.55 10 CFR 73.54 E.5	Yes-
R5	10 CFR 73.55 – physical security rule	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.55 10 CFR 73.54 E.5	Yes-
R6	10 CFR 73.55 – physical security rule	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.55 10 CFR 73.54 E.5	Yes-
R7	10 CFR 73.55 (q)(2)– physical security rule requires records to be kept until license is superseded plus 3 years	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.54 and 55 10 CFR 73.54 E.5	Yes-

CIP 006-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R8	10 CFR 73.55(n) – maintenance of security systems 10 CFR 73.55 (q)(2)– physical security rule requires records to be kept until license is superseded plus 3 years	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 50, 10 CFR 73.54, 73.55 A.4.4, A.4.5 E.3.5, 3.4, E.10	Yes-
R8.1	10 CFR 73.55 (q)(2)– physical security rule requires records to be kept until license is superseded plus 3 years	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 50, 10 CFR 73.54, 73.55 A.4.4, A.4.5 E.3.6, E.4, E.10	Yes-
R8.2	10 CFR 73.55 (q)(2)– physical security rule requires records to be kept until license is superseded plus 3 years	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.55 10 CFR 73.54 (h) A.4.13	Yes-
R8.3	10 CFR 73.55 (q)(2)– physical security rule requires records to be kept until license is superseded plus 3 years 10 CFR 50.59 –	10 CFR 73.55 – physical security rule.	Yes- Part of the existing physical security (protective) plan.	10 CFR 73.55 10 CFR 73.54 (h) A.4.13	Yes-

CIP 006-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	license condition				

Systems Security Management

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R1	10 CFR 50.59 – license condition 10 CFR 73.54 – high assurance of adequate protection	Appendix B.5.5 Installing Operating Systems, Applications and Third-Party Software Updates C.4.1 Continuous Monitoring and Assessment C.4.1.1 Ongoing Assessments of Security Controls C.4.1.2 Effectiveness Analysis of Security Controls C.4.2 Change Control	Yes-	10 CFR 50, 10 CFR 73.54 A.4.4, A.4.5 E.3.6, E.4, E.10	Yes-
R1.1	10 CFR 73.58 – safety security interface 10 CFR 73.54 – high assurance of adequate	C.4.2.2 Security Impact Analysis	Yes-	10 CFR 50, 10 CFR 73.54 A.4.4, A.4.5 E.4, E.10	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	protection 10 CFR 50.59 – license condition – the licensees CSP commits to perform this				
R1.2	10 CFR 50.59 – license condition	Appendix B.5.5 Installing Operating Systems, Applications and Third-Party Software Updates	Yes-	10 CFR 50, 10 CFR 73.54 A.4.4, A.4.5 E.4, E.10	Yes-
R1.3	10 CFR 50.59 – license condition 10 CFR 73.54 (d)(3) – changes have to be tested to ensure they do not adversely effect security	A.4.2.5 Review and Validation Testing of a Modification or Addition of a CDA	Yes-	10 CFR 50, 10 CFR 73.54 A.4.4, A.4.5 E.4, E.10	Yes-
R2	10 CFR 50.59- license condition 10 CFR 73.54 (c) – defense in depth 10 CFR 73.54(d)(3) – changes have to be tested to ensure they do not adversely effect security	Appendix B.5 System Hardening Appendix B.5.1 Removal of Unnecessary Services and Programs	Yes-	D.5, E.6, E.10.8	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R2.1	10 CFR 50.59- license condition 10 CFR 73.54 (c) – defense in depth 10 CFR 73.54(d)(3) – changes have to be tested to ensure they do not adversely effect security	Appendix B.5 System Hardening Appendix B.5.1 Removal of Unnecessary Services and Programs	Yes-	D.5, E.6, E.10.8	Yes-
R2.2	10 CFR 50.59- license condition 10 CFR 73.54 (c) – defense in depth 10 CFR 73.54(d)(3) – changes have to be tested to ensure they do not adversely effect security	Appendix B.5 System Hardening Appendix B.5.1 Removal of Unnecessary Services and Programs	Yes-	D.5, E.6, E.10.8	Yes-
R2.3	10 CFR 50.59- license condition 10 CFR 73.54 (c) – defense in depth 10 CFR 73.54(d)(3) – changes have to be tested to ensure they do not adversely	C.3.3 Security Controls	Yes-	A.3.1.6	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	effect security				
R3	10 CFR 50.59- license condition 10 CFR 73.54 (c) – defense in depth 10 CFR 73.54(d)(3) – changes have to be tested to ensure they do not adversely effect security 10 CFR 73.54(e)(2)(iii) – correct vulnerabilities	Appendix B.5.5 Installing Operating Systems, Applications, and Third-Party Software Updates	Yes-	D.5.1, D.5.5	Yes-
R3.1	10 CFR 50.59- license condition 10 CFR 73.54 (c) – defense in depth 10 CFR 73.54(e)(2)(iii) – correct vulnerabilities 10 CFR 73.54(f) – document Corrective Action Program 10 CFR 73.55(o) – compensatory	Appendix B.5.5 Installing Operating Systems, Applications, and Third-Party Software Updates	Yes-	D.5.1, D.5.5	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	measures must be implemented upon discovery of as vulnerability, weakeness, etc.				
R3.2	10 CFR 50.59- license condition 10 CFR 73.54 (c) – defense in depth 10 CFR 73.54(e)(2)(iii) – correct vulnerabilities 10 CFR 73.54(f) – document Corrective Action Program 10 CFR 73.55(o) – compensatory measures must be implemented upon discovery of as vulnerability, weakness, etc.	Appendix B.5.5 Installing Operating Systems, Applications, and Third-Party Software Updates	Yes-	D.5.1, D.5.5, A.3.1.6	Yes-
R4	10 CFR 50.59 – license condition 10 CFR 73.54 – high assurance of adequate	C.7 Defense in Depth	Yes-	D.5, E.6	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	protection 10 CFR 73.54(c) – defense in depth				
R4.1	10 CFR 50.59 – license condition 10 CFR 73.54 – high assurance of adequate protection 10 CFR 73.54(c) – defense in depth	C.3.3 Malicious Code Protection	Yes-	D.5, E.6	Yes-
R4.2	10 CFR 50.59 – license condition 10 CFR 73.54 – high assurance of adequate protection 10 CFR 73.54(c) – defense in depth	C.3.3 Malicious Code Protection	Yes-	D.5, E.6 Other testing procedures mentioned above.	Yes-
R5	10 CFR 73.54 – high assurance of adequate protection 10 CFR 73.54(c)(2) – respond, detect and recovery from attacks 10 CFR 50.59 – license condition	C.3.3.1.1 Access Control C.3.3.1.2 Audit and Accountability Appendix B.1.1 Access Control Policy and Procedures Appendix B.1.2 Account Management	Yes-	D.1, D.2, D.4	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R5.1	10 CFR 73.54 – high assurance of adequate protection 10 CFR 73.54(c) – defense in depth 10 CFR 50.59 – license condition	Appendix B.1.2 Account Management	Yes-	D.1, D.2, D.4	Yes-
R5.1.1	10 CFR 73.54 – high assurance of adequate protection 10 CFR 73.54(c) – defense in depth 10 CFR 50.59 – license condition	Appendix B.1.1 Access Control Policy and Procedures	Yes-	D.1, D.2, D.4	Yes-
R5.1.2	10 CFR 73.54 – high assurance of adequate protection 10 CFR 73.54(c) – defense in depth 10 CFR 50.59 – license condition 10 CFR 73.54(f) – records kept for at least a year	Appendix B.1.2 Account Management	Yes-	D.1, D.2, D.4, D.5, E.6	Yes-
R5.1.3	10 CFR 73.55 – review access every	Appendix B.1.2 Account	Yes-	D.1, D.4	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	31 days	Management			
R5.2	10 CFR 50.59 10 CFR 73.54	C.3.3.1.5 System Hardening	Yes-	D.1, D.5.3	Yes-
R5.2.1	10 CFR 73.56 (b)(4)(i) 10 CFR 50.59 license condition	Appendix B.1.2 Account Management	Yes-	D.1, D.5, E.6	Yes-
R5.2.2	10 CFR 73.56 (b)(4)(i) 10 CFR 50.59 license condition 10 CFR 73.54	C.3.3.1.1 Access Control	Yes-	D.4.2	Yes-
R5.2.3	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 73.54© - defense in depth 73.54 (h) – records must be kept at least a year	C.3.3.1.1 Access Control	Yes-	D.4.2	Yes-
R5.3	10 CFR 50.59 license	Appendix B.4.3 Password	Yes-	D.4.3	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	condition 10 CFR 73.54(a) – high assurance of adequate protection 73.54(c) - defense in depth	Requirements Appendix B.4.7 Authenticator Management			
R5.3.1	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 73.54(c) - defense in depth This is determined in inspection	Appendix B.4.3 Password Requirements	Yes-	Specified based on technical feasibility and level of protection required.	Yes-
R5.3.2	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 73.54(c) - defense in depth This is determined in inspection	Appendix B.4.3 Password Requirements	Yes-	Specified based on technical feasibility and level of protection required.	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R5.3.3	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 73.54(c) - defense in depth	Appendix B.4.3 Password Requirements	Yes-	92d	Yes-
R6	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 73.54(c) - defense in depth 73.54 (e)(2)(i) – maintain timely ability do detect and respond to cyber attacks	C.3.1 System and Information Integrity Policy and Procedures C.3.4 Monitoring Tools and Techniques Appendix B.5.2 Host Intrusion Detection System	Yes-	A.4.2, A.4.4	Yes-
R6.1	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 73.54(c) - defense in depth	C.8.5. Incident Monitoring Appendix C.3.4 Monitoring Tools and Techniques	Yes-	D.2.6	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	73.54 (e)(2)(i) – maintain timely ability do detect and respond to cyber attacks				
R6.2	73.54 (e)(2)(i) – maintain timely ability do detect and respond to cyber attacks 73.54(h) – records must be maintained for at least one year	Appendix C.8.5. Incident Monitoring	Yes-	E.6	Yes-
R6.3	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 73.54(c) - defense in depth	Appendix B.2.2 Auditable Events	Yes-	10 CFR 73.54 (h), A.4.13	Yes-
R6.4	73.54(h) – records must be maintained for at least one year	Appendix B.2.11 Audit Record Retention	Yes-	10 CFR 73.54 (h), A.4.13	Yes-
R6.5	10 CFR 50.59 license condition	Appendix C.8 Incident Response	Yes-	D.2.6	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	10 CFR 73.54(a) – high assurance of adequate protection 73.54(c) - defense in depth 73.54 (e)(2)(i) – maintain timely ability do detect and respond to cyber attacks 10 CFR 50.59 – corrective action program Appendix G of Pary 73 requires reporting to NRC within 1 hour of certain events, attacks, uncompensated vulnerabilities	Appendix C.8.4 Incident Handling			
R7	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 10 CFR 73.54 (d)(3) – modifications and	Appendix C.1.1 Media Protection Policy and Procedures Appendix C.1.6 Media Sanitation and Disposal	Yes-	E.1.1, E.1.6	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	additions must be evaluated for security impact before changes are made to ensure there is no adverse impact 73.54(c) - defense in depth				
R7.1	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 10 CFR 73.54 (d)(3) – modifications and additions must be evaluated for security impact before changes are made to ensure there is no adverse impact 73.54(c) - defense in depth	Appendix C.1.6 Media Sanitation and Disposal	Yes-	E.1.1, E.1.6	Yes-
R7.2	10 CFR 50.59 license	Appendix C.1.6 Media	Yes-	E.1.1, E.1.6	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	condition 10 CFR 73.54(a) – high assurance of adequate protection 10 CFR 73.54 (d)(3) – modifications and additions must be evaluated for security impact before changes are made to ensure there is no adverse impact 73.54(c) - defense in depth	Sanitation and Disposal			
R7.3	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 10 CFR 73.54 (d)(3) – modifications and additions must be evaluated for security impact before changes are made to ensure there is no	Appendix C.1.1 Media Protection Policy and Procedures	Yes-	10 CFR 73.54 (h) A.4.13	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	adverse impact 73.54(c) - defense in depth				
R8	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 10 CFR 73.54 (d)(3) – modifications and additions must be evaluated for security impact before changes are made to ensure there is no adverse impact 73.54(c) - defense in depth	C.3.1.2 Define Roles and Responsibilities and Form the Cyber Security Team C.3.3 Security Controls C.4 Maintaining the Cyber Security Program C.4.1.3 Vulnerability Scans and Assessments	Yes-	A.4.4.3.2 E.12	Yes-
R8.1	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 10 CFR 73.54 (h) – records must be	C.3.2 Flaw Remediation	Yes-	A.4.4.3.2 E.12	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	maintained for at least one year				
R8.2	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 10 CFR 73.54 (h) – records must be maintained for at least one year	C.4.1.1 Ongoing Assessments of Security Controls	Yes-	A.4.4.3.2 E.12	Yes-
R8.3	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 10 CFR 73.54 (h) – records must be maintained for at least one year	Appendix B.1.2 Account Management	Yes-	D.4.1	Yes-
R8.4	10 CFR 50.59 license condition 10 CFR 73.54(a) – high assurance of adequate protection 10 CFR 73.54 (h) –	C.3.2 Flaw Remediation	Yes-	10 CFR 73.54 (h) A.4.4.3.2 Corrective Action program	Yes-

CIP 007-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	records must be maintained for at least one year 10 CFR 73.54(e)(2)(iii) Corrective Action Program				
R9	73.55(m) – security plan review requirements 10 CFR 50.59 license condition 10 CFR 73.54(d)(3) – changes must be documented and analyzed for adverse impact on security 10 CFR 73.54 (h) – records must be maintained for at least one year	C.4.3 Cyber Security Program Review	Yes-	10 CFR 73.54(g) A.4.12	Yes-

Incident Reporting and Response Planning

CIP 008-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R1	10 CFR 73.54 (e)(2) – incident response plan	C.3.3.2.6 Incident Response	Yes-	A.4.6, E.7, E.8	Yes-
R1.1	10 CFR 73 appendix G – reporting of security events	C.8.1 Incident Response Policy and Procedures	Yes-	E.7.4	Yes-
R1.2	10 CFR 73.54 (e)(2) – incident response plan 73.55 Safeguards contingency plan	C.3.3.2.6 Incident Response C.8.4 Incident Handling	Yes-	E.7.1	Yes-
R1.3	10 CFR 73 appendix G – reporting of security events Licensee reports to NRC per Appendix G, Responsibility of notifying other plants belongs to the NRC	C.8.6 Incident Reporting	Yes-	10 CFR 73.71	Yes-
R1.4	10 CFR 50.59 – changes are approved by the NRC	10 CFR 50.59 – changes are approved by the NRC	Yes- Addressed by the plant change management program.	10 CFR 73.54 (m) sets maximum review of 2 years. May be revised as licensee desires.	Yes-
R1.5	10 CFR 50.59 –	C.8.8 Cyber Incident	Yes-	10 CFR 73.54 (m)	Yes-

CIP 008-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	license condition RG 5.71 requires annually, however a licensee can take exception to this – but this exception can exceed every 24 months	Response Plan		sets maximum review of 2 years. May be revised as licensee desires.	
R1.6	10 CFR 50.59 – license condition RG 5.71 requires annually, however a licensee can take exception to this – but this exception can exceed every 24 months	C.8.2 Incident Response Training C.8.3 Incident Response Testing and Drills	Yes-	E.7.2	Yes-
R2	10 CFR 73 Appendix G – reporting of cyber events and attacks 10 CFR 73.54(h) – records must be kept for the duration of the licensee, plus 3 years	C.5 Records Retention and Handling	Yes-	10 CFR 73.54 (h) A.4.13	Yes-

Recovery Plans for Critical Cyber Assets

CIP 009-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R1	10 CFR 73.54 (e)(2) – Requires recovery plan RG 5.71 requires annually, however a licensee can take exception to this – but this exception can exceed every 24 months	C.8.1 Incident Response Policy and Procedures C.3.3.2.7 Contingency Planning/Continuity of SSEP Functions	Yes-	NRC Technical Specifications A.4.6, E.7, E.8	Yes-
R1.1	10 CFR 73.54 (e)(2) – Requires recovery plan RG 5.71 requires annually, however a licensee can take exception to this – but this exception can exceed every 24 months 10 CFR 73 Appendix C – Safeguards contingency plan	C.9.1 Contingency Planning Policy and Procedures	Yes-	A.4.6, A.4.7	Yes-
R1.2	10 CFR 50.59 – license condition RG 5.71 requires annually, however a	C.3.3.2.7 Contingency Planning/Continuity of SSEP Functions	Yes-		

CIP 009-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
	licensee can take exception to this – but this exception can exceed every 24 months 10 CFR 73 Appendix C – Safeguards contingency plan				
R2	10 CFR 50.59 – license condition RG 5.71 requires annually, however a licensee can take exception to this – but this exception can exceed every 24 months 10 CFR 73 Appendix C – Safeguards contingency plan	C.8.1 Incident Response Policy and Procedures C.8.3 Incident Response Testing and Drills	Yes-	E.7.2, E.8.3	Yes-
R3	10 CFR 50.59 – license condition 10 CFR 73.55 (o) – must compensate for weaknesses when discovered	C.8.1 Incident Response Policy and Procedures	Yes-	E.7.1,	Yes-

CIP 009-3 Requirement	Section(s) in NRC Rules	Section(s) in RG 5.71 or applicable NRC rule(s)	Does RG 5.71 provide adequate controls or other controls?	Section(s) in NEI 08-09 or applicable NRC rule(s)	Does NEI 08-09 provide adequate controls or other controls?
R4	10 CFR 50.59 – license condition 10 CFR 73.54 (e)(2)(iv) – License must be able to restore and recover	C.8.1 Incident Response Policy and Procedures C.9.5 Alternate Storage Site and Location for Backups C.9.6. CDA Backups C.9.7 Recovery and Reconstitution	Yes-	E.8.5, E.8.6	Yes-
R5	10 CFR 50.59 – license condition 10 CFR 73.54 (e)(2)(iv) – License must be able to restore and recover	C.9.6. CDA Backups	Yes-	E.8.5, E.8.6	Yes-

Contributors/ Subject Matter Experts to this report

NERC	Tim Roxey
NERC	Jim Hughes
FERC	Redacted
NRC	Redacted
NRC	Redacted
NRC	Redacted
NEI	Redacted