NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

September 15, 2009

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation ("NERC") hereby submits this Compliance Filing and Petition for Approval, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA") and Part 39.5 of the Federal Energy Regulatory Commission's ("FERC") regulations, an implementation plan for Generator Owners and Generator Operators of nuclear power plants in the United States for Version 1 of the Critical Infrastructure Protection Reliability Standards, CIP-002-1 through CIP-009-1 ("Implementation Plan"), as set forth in **Exhibit A** to this petition. This filing is being made in compliance with FERC's directive in Paragraph 60 of Order No. 706-B[1] directing "the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards."[2] FERC directed NERC to "submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."[3]

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 126 FERC ¶ 61,229 (2009) (Order No. 706-B).
[2] *Id.* at P 60.
[3] *Id.*

The proposed Implementation Plan was approved by the NERC Board of Trustees on September 14, 2009. NERC requests that the Implementation Plan take effect immediately upon FERC approval, and that the CIP-002-1 through CIP-009-1 Reliability Standards become mandatory and enforceable upon Generator Owners and Generator Operators of nuclear power plants in the United States in accordance with the provisions contained in the Implementation Plan. Upon FERC's approval of Version 2 of the CIP-002 through CIP-009 Reliability Standards, which were filed with FERC for approval on May 22, 2009, NERC respectfully requests that FERC require the approved Version 2 Reliability Standards to be implemented by U.S. nuclear power plant owners and operators on a schedule no sooner than that included in the Implementation Plan that is the subject of this filing.

This petition consists of the following:

- this transmittal letter;
- a table of contents for the entire petition;
- the Implementation Plan for CIP-002-1 through CIP-009-1 for Generator Owners and Generator Operators of U.S. Nuclear Power Plants submitted for approval (**Exhibit A**);
- the Record of Development of the Proposed Implementation Plan for CIP-002-1 through CIP-009-1 for Generator Owners and Generator Operators of U.S. Nuclear Power Plants (**Exhibit B)**; and
- the Standard Drafting Team roster (**Exhibit C**).

Please contact the undersigned if you have any questions.

Respectfully submitted,

/s/ Holly A. Hawkins
Holly A. Hawkins

Attorney for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMPLIANCE FILING AND PETITION FOR APPROVAL OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF AN IMPLEMENTATION PLAN FOR CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS FOR GENERATOR OWNERS AND GENERATOR OPERATORS OF U.S. NUCLEAR POWER PLANTS IN ACCORDANCE WITH PARAGRAPH 60 OF ORDER NO. 706-B

Rick Sergel
President and Chief Executive Officer
David N. Cook
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

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

September 15, 2009

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMPLIANCE FILING AND PETITION FOR APPROVAL OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF AN IMPLEMENTATION PLAN FOR CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS FOR GENERATOR OWNERS AND GENERATOR OPERATORS OF U.S. NUCLEAR POWER PLANTS IN ACCORDANCE WITH PARAGRAPH 60 OF ORDER NO. 706-B

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[4] hereby requests the Federal Energy Regulatory Commission ("FERC") to approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[5] and Section 39.5 of FERC's regulations, 18 C.F.R. § 39.5, an implementation plan for Critical Infrastructure Protection ("CIP") Reliability Standards, CIP-002-1 through CIP-009-1 for Generator Owners and Generator Operators of U.S. nuclear power plants ("Implementation Plan"), included in **Exhibit A** of this petition.

The proposed Implementation Plan will be in effect only within the United States. This petition is for approval of a new Implementation Plan, in response to FERC's

[4] NERC has been certified by FERC as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act. FERC certified NERC as the ERO in its order issued July 20, 2006, in Docket No. RR06-1-000. *North American Electric Reliability Corporation*, "Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing," 116 FERC ¶ 61,062 (2006) ("ERO Certification Order).
[5] 16 U.S.C. 824o.

directive in Order No. 706-B[6] issued on March 19, 2009, that will apply to Generator Owners and Generator Operators of U.S. nuclear power plants.[7] In Order No. 706-B, FERC stated in paragraphs 59 to 60:

> it is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan,[8] i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule.

On September 14, 2009, the NERC Board of Trustees approved this Implementation Plan that will specifically apply to Generator Owners and Generator Operators of U.S. nuclear power plants for NERC CIP Reliability Standard compliance by an action in writing without a meeting. NERC requests that FERC approve this Implementation Plan and make it effective immediately upon approval. The CIP-002-1

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

[7] In Order No. 706, FERC approved the currently in-force Implementation Plan now codified in Appendix 3A of NERC's Rules of Procedure. *See Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) (Order No. 706). This Implementation Plan applies to all entities subject to NERC CIP Reliability Standards except Generator Owners and Generator Operators of nuclear power plants in the U.S. Those specific entities will be covered by the Implementation Plan currently being proposed in this filing.

[8] The referenced Implementation Plan was originally proposed by NERC when it submitted the original set of Critical Infrastructure Protection standards in August, 2006. The plan was approved by the Commission in January 2008, when it approved the CIP-002-1 through CIP-009-1 Reliability Standards. According to the approved plan, Generator Owners are to be compliant with the CIP Reliability Standards in December 2009. Nuclear Power Plant owners believed they were exempt from the NERC CIP standards based on language contained in the Applicability section of the standard. However, the Commission in Order No. 706-B clarified that the CIP standards also applied to Generator Owners and Generator Operators of U.S. nuclear power plants for balance of plant systems.

through CIP-009-1 requirements will become mandatory and enforceable on Generator Owners and Generator Operators of U.S. nuclear plants in accordance with the provisions in the Implementation Plan. Additionally, on May 22, 2009, NERC filed the Version 2 of the CIP-002 through CIP-009 Reliability Standards for FERC approval. Upon FERC's approval of Version 2 of the CIP Reliability Standards, NERC respectfully requests that FERC require the approved Version 2 Reliability Standards to be implemented by U.S. nuclear power plant owners and operators on a schedule no sooner than that included in the Implementation Plan that is the subject of this filing.

Exhibit A to this filing sets forth the proposed Implementation Plan. **Exhibit B** contains the complete record of development for the proposed plan. **Exhibit C** includes the standard drafting team roster.

II. NOTICES AND COMMUNICATIONS

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

Rick Sergel
President and Chief Executive Officer
David N. Cook
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.

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

III. BACKGROUND

a. Regulatory Framework

By enacting the Energy Policy Act of 2005,[9] 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 ERO that will be charged with developing and enforcing mandatory Reliability Standards, subject to FERC approval. Section 215 of the FPA states that all users, owners and operators of the bulk power system in the United States will be subject to FERC-approved Reliability Standards.

b. Basis for Approval of Proposed Implementation Plan

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

> The Commission may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest.[10]

When evaluating proposed Reliability Standards or modifications to proposed Reliability Standards, FERC is expected to give "due weight" to the technical expertise of the ERO and to the technical expertise of a Regional Entity organized on an

[9] 16 U.S.C. § 824o.
[10] 16 U.S.C. § 824o(d)(2).

Interconnection-wide basis with respect to a Reliability Standard to be applicable within that Interconnection. Order No. 672 provides guidance on the factors FERC will consider when determining whether proposed Reliability Standards meet the statutory criteria.[11] Because the Implementation Plan proposed in this filing is a required element in the development of a Reliability Standard, NERC developed this Implementation Plan using the same procedure it would use to develop a Reliability Standard. NERC's procedure requires that the proposed Implementation Plan be posted for at least one public comment period and be approved as part of the ballot of the Reliability Standard.

c. Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC *Reliability Standards Development Procedure*, which is incorporated into the Rules of Procedure as Appendix 3A. In its ERO Certification Order, FERC found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the bulk power system. NERC considers the comments of all stakeholders, and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard for submission to FERC.

The proposed Implementation Plan included in **Exhibit A** has been developed and approved by industry stakeholders using NERC's *Reliability Standards Development*

[11] *See Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards,* 114 FERC ¶ 61,104 (2006) at PP 320-338 ("Order No. 672"), *order on reh'g,* 114 FERC ¶ 61,328 (2006) ("Order No. 672-A").

Procedure, and it was approved by the NERC Board of Trustees on September 14, 2009 for filing with FERC.

IV. SUMMARY OF THE IMPLEMENTATION PLAN DEVELOPMENT PROCEEDINGS

NERC decided to reinstate the willing members of the standard drafting team that developed the first version of the CIP Reliability Standards approved by FERC in Order No. 706 in January 2008. The original roster of drafting team members is included in **Exhibit C** to this filing. Reconstituted in June 2009, the team, supplemented by several participants from the U.S. nuclear community, including the Nuclear Energy Institute, benefited from the NERC "Town Hall Meeting" conducted in Toronto, Ontario on June 11, 2009, to discuss implementation issues with industry stakeholders relative to Order No. 706-B. The team, in its deliberations on the proposed Implementation Plan, was faced with several key issues. The first was the belief of nuclear power plant owners that all systems, structures, and components were already under the jurisdiction of the Nuclear Regulatory Commission ("NRC").

The second was the recognition that significant uncertainty existed regarding the outcome of the NERC-NRC discussions on the Memorandum of Understanding under development at the time the Implementation Plan was being contemplated – in particular, there was ambiguity regarding how NERC will process and evaluate requests for exemption from compliance with NERC's CIP Reliability Standard requirements for systems, structures, and components identified to be within NERC's jurisdiction. That is, an entity will be able to apply for exemption from compliance with NERC's CIP Reliability Standards if it believes that a specific component within the balance of plant is more appropriately subject to NRC cyber security regulations, thereby avoiding "dual

regulation" as contemplated in Paragraph 50 of Order No. 706-B (the "Exemption Process"). The team believed that the availability of the Exemption Process needed to be acknowledged in the Implementation Plan.

Third, the team determined that the timing of the Implementation Plan for NERC's CIP standards should be commensurate with implementation of the NRC's cyber security regulations for systems, structures, and components within its jurisdiction. Fourth, because of the rigor of the nuclear unit planned-outage schedule, the implementation plan needed to take into account the possibility that certain of the requirements could not be implemented without the nuclear plant going out of service, and therefore, sufficient time needed to be made available to properly plan, schedule, and budget for the nuclear outage-related activities. Finally, the outage-related timeframes needed to include sufficient time following the outage to complete the documentation requirements for the implemented change.

In response to these challenges, the team determined a course of action in developing the Implementation Plan that was predicated upon three main factors, or critical path items, that determined an appropriate timeframe for compliance with NERC CIP Reliability Standards. First, for requirements that are not outage-dependent, the Implementation Plan requires compliance within 18 months following the FERC effective date of the Implementation Plan. The team recognized that significant preparatory work has already been undertaken to address cyber security at U.S. nuclear power plants. Further, nuclear power plant owners are required by the NRC to submit a comprehensive cyber security plan for each plant by November 2009, in accordance with recently enacted NRC regulations, that will then need to be evaluated and accepted by the

NRC for implementation at the plant. The timing of the proposed Implementation Plan provides a reasonable timeframe in which entities can plan and implement the needed requirements in the context of their NRC cyber security plans.

The second critical path item affecting an appropriate timeframe for compliance included in the Implementation Plan is the availability of the Exemption Process (*i.e.* the determination of which specific components fall within NERC's jurisdiction and which specific components fall within the NRC's jurisdiction). This delineation of specific components, as well as a process detailing how an entity is to request an exemption from NERC jurisdiction, is expected to be provided in the final Memorandum of Understanding currently being developed between NERC and the NRC. The team determined that the Memorandum of Understanding detailing this process between NERC and the NRC must be finalized before an entity can fully determine its obligations under NERC's CIP Reliability Standards. Accordingly, the team included in the Implementation Plan the possibility that the availability of an agreed-upon Memorandum of Understanding could be a limiting factor in terms of achieving compliance with the NERC CIP Reliability Standards. Therefore, the team developed the Implementation Plan, recognizing that the timeframe for compliance should be based upon the latter of the FERC approval date plus a certain timeframe, typically 18 months, or the date that the Memorandum of Understanding is agreed to between NERC and the NRC, thereby providing a system in which to determine an entities' requested exception from NERC compliance, plus 10 months.

Third, the team acknowledged that certain of the NERC CIP Reliability Standards requirements were likely predicated upon a nuclear unit outage to be fully implemented.

Because of the rigorous schedule for nuclear unit outages, it was apparent that for those requirements dependent on an outage to implement the NERC CIP Reliability Standards, accommodations in the timeframe for implementation were required to properly plan, budget, and schedule the changes or modifications during a refueling outage. The team also considered the expectation that final documentation of such outage-related modifications would follow after the outage itself was completed. Thus, the team permitted an additional approach for those requirements identified as outage-dependent. The development of supporting processes and procedures is still expected within the latter of the FERC effective date plus 18 months, or the execution date of the Memorandum of Understanding (that includes the scope of systems determination and the Exemptions Process) plus 10 months. However, for those requirements that require a unit outage to be implemented, the team determined the timeline for compliance to be 6 months after the completion of the first refueling outage that is at least 18 months following the FERC effective date. This approach meets the concerns of nuclear power plant owners regarding the time necessary to properly plan, budget, schedule, and implement requirements that are outage-dependent, and will provide the time needed to finalize the documentation of such "as-built" changes following the outage.

In summary, the Implementation Plan requires compliance with the CIP Reliability Standards by the later of the FERC effective date plus 18 months, or the Memorandum of Understanding execution date plus 10 months. For requirements that are outage-dependent, the Implementation Plan requires compliance with the CIP Reliability Standards within 6 months after the completion of the first refueling outage that is at least 18 months following the FERC effective date.

The proposed Implementation Plan was posted for industry comment from July 20, 2009 through August 14, 2009.[12] In accordance with NERC Standards Committee action, this period also served concurrently as the pre-ballot review period. There were 15 sets of comments, including comments from more than 40 people from approximately 25 companies representing seven of the ten industry segments. The majority of the stakeholders supported the approach taken but indicated concern in three key areas: that the implementation timeframe for requirements tied to refueling outages was not sufficient; that additional requirements, particularly those in CIP-006-1, could be dependent upon an outage to be fully implemented; and that the scope of systems determination and the Exemption Process should include the time to evaluate and dispose of an exemption request.

Upon consideration, the drafting team added CIP-006-1 to the list of standards potentially requiring an outage to be implemented. Additionally, the team agreed with commenters that the Implementation Plan for requirements dependent upon a refueling outage was confusing. Because the Implementation Plan could not be implemented any sooner than the FERC effective date plus eighteen months, the team agreed to modify the implementation plan for requirements requiring an outage to be implemented to six months following the first refueling outage, at least 18 months following the FERC effective date. The team did not agree that the Exemptions Process should include the time needed to invoke and receive disposition of an exemption request. The Exemptions

[12] The team requested and received approval from the NERC Standards Committee to adjust several process steps to enable the team to complete the implementation plan ballot period by the September 15, 2009 FERC filing date. At its July 15-16, 2009 meeting, the Standards Committee approved a motion to permit the team to modify the Implementation Plan in response to comments and to proceed directly to the ballot phase. Under the *Reliability Standards Development Procedure*, if substantive modifications are made to the Implementation Plan, the plan should be presented for another period for industry review. Also, the Standards Committee agreed to conduct the industry comment period and the pre-ballot review period concurrently, another departure from common practice.

Process will build in the time needed for the determination on whether an exemption should be granted. In this regard, NERC realizes the need to expeditiously respond to requests for exemptions to ensure that the implementation of the CIP Reliability Standards takes place efficiently.

In accordance with the NERC Standards Committee's decision to permit the team to modify the Implementation Plan and proceed to the ballot phase without presenting the plan for further industry comment, the drafting team modified the Implementation Plan in the two areas discussed above and began the balloting period. The initial 10-day ballot period began on August 19, 2009, and concluded on August 28, 2009. The ballot achieved a weighted segment approval percentage of 97.37 percent, beyond the two-thirds necessary for passage. A quorum of 81.96 percent of the ballot pool voted, exceeding the 75 percent needed for a valid ballot. There was one negative vote accompanied by comments and eight affirmative votes with comments attached.

The comments centered around three main themes, each of which was addressed during the industry comment period. The first concern was the desire to have the invocation of the exemption process and disposition of the request included in the timeframe linked to the Memorandum of Understanding and scope of systems determination therein. As noted previously, the team does not agree with this approach. The second concern pertained to the timeframe associated with outage-dependent requirements being too short, identified by the commenter as the FERC effective date plus 12 months. The team already extended this timeframe to the FERC effective date plus 18 months for these requirements prior to the initiation of the ballot. Last, commenters were concerned about certain requirements in CIP-006-1 and CIP-007-1 not

being properly labeled as outage-dependent. The team also addressed these prior to the start of balloting. As a result of these comments, the team made no further changes to the Implementation Plan.

Because a negative vote was presented with a comment, the team conducted a recirculation ballot that took place from September 1, 2009 through September 10, 2009. The Implementation Plan achieved a final approval percentage of 97.18 percent, with 87.11 percent of the ballot pool voting. The NERC Board of Trustees approved the Implementation Plan on September 14, 2009.

VI. CONCLUSION

NERC requests that FERC approve the proposed Implementation Plan for CIP-002-1 through CIP-009-1 for Generator Owners and Generator Operators of U.S. nuclear power plants and make the plan effective immediately, pursuant to section 215(d) of the FPA, and in response to the directives contained in Order No. 706-B. Additionally, upon FERC's approval of Version 2 of the CIP-002 through CIP-009 Reliability Standards, NERC respectfully requests that FERC require the approved Version 2 Reliability Standards to be implemented by U.S. nuclear power plant owners and operators on a schedule no sooner than that included in the Implementation Plan that is the subject of this filing.

Respectfully submitted,

/s/ Holly A. Hawkins

Rick Sergel
President and Chief Executive Officer
David N. Cook
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

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

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 15th day of September, 2009.

/s/ Holly A. Hawkins
Holly A. Hawkins

Attorney for North American Electric Reliability Corporation

Exhibit A

Implementation Plan for CIP-002-1 through CIP-009-1
For Generator Owners and Generator Operators of
U.S. Nuclear Power Plants

Implementation Plan Purpose

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the Critical Infrastructure Protection Reliability Standards, CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "that the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

Implementation Plan Scope

This implementation plan focuses solely on the implementation of the following standards as they apply to nuclear power plants owners and operators:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

Prerequisite approvals or activities

1. FERC must approve the implementation plan for it to take effect. This FERC approved effective date is referenced in the implementation table by the label "R", signifying the date the Order takes effect.
2. The specific systems, structures, and components must be identified regarding the regulatory jurisdiction in which it resides in order to determine whether NERC CIP standards must be applied. This scope of systems determination, reflected by the label "S", includes the completion of an executed Memorandum of Understanding between

NERC and the NRC on this and other related issues. The scope of system determination also requires the establishment of the exemption process for excluding certain systems, structures, and components from the scope of NERC CIP standards as provided for in Order 706-B.

3. Certain of the NERC CIP standards can only be implemented with the unit off-line. Therefore, certain requirements are likely outage-dependent and are so identified by the label "RO". These items need to be included in the plant's "checkbook" indicated they are planned and budgeted for as part of the planned outage activities. In this context, the refueling outage refers to the first refueling outage at least 18 months beyond the FERC effective date to provide the time needed to plan and budget the activities.

   Specifically, aspects of CIP-005-1, CIP-006-1, CIP-007-1, and CIP-008-1 requirements pertaining to the **development** of plans, processes, and protocols shall be completed the later of FERC Effective Date ("R") +18 months or Scope of Systems Determination ("S") +10 months. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or six months following the completion of the first refueling outage at least 18 months following the FERC Effective Date ("RO")if an outage is required to implement the plans, processes, and protocols. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in the self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in the self-certification report, including the time frame needed for implementation for each unit.

Each of these factors can become the critical path item that determines an appropriate timeline for compliance; therefore, the proposed plan is structured that the timeline for compliance becomes the later of:

- the FERC Effective Date plus 18 months;
- the Scope of Systems Determination plus 10 months; or,
- six months following the completion of the first refueling outage (if applicable) at least 18 months following the FERC Effective Date. The added six months enables the entity to complete the documentation requirements for the implemented changes.

List of functions that must comply with this implementation plan[1]

- Nuclear Generator Owners
- Nuclear Generator Operators

[1] Note that the CIP standards apply to many additional functional entities – and there is a separate implementation plan, already approved by FERC and other regulatory authorities, that applies to those other functional entities.

CIP-002-1 — Critical Cyber Asset Identification			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	No	R+12 months
R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	No	R+12 months
R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	No	Later of: • R+18 months, or • S+10 months
R4.	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-003-1 — Security Management Controls			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009	No	Later of: • R+18 months, or • S+10 months
R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	No	Later of: • R+18 months, or • S+10 months
R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months
R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	No	Later of: • R+18 months, or • S+10 months
R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

CIP-004-1 — Personnel and Training			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: Direct communications (e.g., emails, memos, computer based training, etc.); Indirect communications (e.g., posters, intranet, brochures, etc.); Management support and reinforcement (e.g., presentations, meetings, etc.).	No	Later of: • R+18 months, or • S+10 months
R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	No	Later of: • R+18 months, or • S+10 months
R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	No	Later of: • R+18 months, or • S+10 months
R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-005-1 — Electronic Security Perimeters

Aspects of requirements of CIP-005-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-006-1 — Physical Security of Critical Cyber Assets

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	Possible	Later of: • R+18 months, or • S+10 months, or

			• RO+6 months (if applicable)
R6.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Account Management — The Responsible Entity shall establish, implement, and	Possible	Later of:

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
	document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.		• R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R7.	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-008-1 — Incident Reporting and Response Planning

Aspects of requirements of CIP-008-1 pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-009-1 — Recovery Plans for Critical Cyber Assets			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	No	Later of: • R+18 months, or • S+10 months
R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	No	Later of: • R+18 months, or • S+10 months
R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	No	Later of: • R+18 months, or • S+10 months
R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

Exhibit B

Record of Development of Proposed Implementation Plan

Cyber Security – Order 706B Nuclear Plant Implementation Plan

Status

A recirculation ballot window for an implementation plan for Version 1 critical infrastructure protection (CIP) Reliability Standards CIP-002-1 through CIP-009-1 for Nuclear Power Plants is now open until 8 p.m. EDT on September 10, 2009.

In order to be responsive to the September 15, 2009 filing deadline and as a reflection of the significant involvement of the nuclear community in the development of this proposal, the NERC Standards Committee approved the team to shorten the comment period and pre-ballot review period, and if necessary, offer changes to the proposal based on the comments received before proceeding to ballot.

Purpose / Industry Need

In Order 706-B, FERC provided the following determination:

> 59. The Commission finds that it is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> 60. Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule.

Proposed Standard	Comment Period	Comments Received	Response to Comments
Announcement **(12)** Order 706-B Nuclear Implementation Plan for CIP Standards Posted for a 10-day Recirculation Ballot Implementation Plan Clean **(13)** | Redline **(14)**	09/01/09 - 09/10/09 (closed) Recirculation Ballot		Announcement **(15)** Ballot Results **(16)**
Announcement **(6)** Order 706-B Nuclear Implementation Plan for CIP Standards Posted for a 10-day Initial Ballot Window Implementation Plan Clean **(7)** | Redline **(8)**	08/19/09 - 08/28/09 (closed) Ballot		Announcement **(9)** Initial Ballot Results **(10)** Consideration of Comments **(11)**
Announcement **(1)** Order 706-B Nuclear Implementation Plan for CIP Standards Posted for a Shortened Comment Period and Pre-ballot Review Period Implementation Plan **(2)**	07/20/09 - 08/14/09 (closed) Electronic Comment Form **(same as 3)** Join Ballot Pool Unofficial Word Version **(3)**	Comments Received **(4)**	Consideration of Comments **(5)**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Pool and Pre-ballot Window (with Comment Period)
July 20–August 14, 2009

Ballot Pool: https://standards.nerc.net/BallotPool.aspx

Comments:
http://www.nerc.com/filez/standards/Cyber_Security_Order706B_Nuclear_Plant_Implementation_Plan.html

Cyber Security — Order 706B Nuclear Plant Implementation Plan

A draft implementation plan for Version 1 critical infrastructure protection (CIP) Reliability Standards CIP-002-1 through CIP-009-1 for Nuclear Power Plants has been posted for a simultaneous pre-ballot review and comment period.

In order to be responsive to the September 15, 2009 filing deadline and as a reflection of the significant involvement of the nuclear community in the development of this proposal, the NERC Standards Committee approved the team to shorten the comment period and hold the comment period at the same time as the pre-ballot review period, and if necessary, offer changes to the proposal based on the comments received before proceeding to ballot.

Ballot Pool

Registered Ballot Body members may join the ballot pool to be eligible to vote on this interpretation **until 8 a.m. EDT on August 14, 2009**.

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list server for this ballot pool is: bp-Order706B_ImpPlan_in.

Comments

An associated comment period is open **until 8 a.m. EDT on August 14, 2009**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Lauren Koller at Lauren.Koller@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page:

http://www.nerc.com/filez/standards/Cyber_Security_Order706B_Nuclear_Plant_Implementation_Plan.html

Project Background:

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the CIP Reliability Standards: CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

This project addresses the development of the implementation plan specific for nuclear power plants. The draft plan was drafted by members of the original Version 1 Cyber Security Drafting Team with specific outreach to nuclear power plant owners and operators to ensure their interests were fairly represented. Further background information is available in the posted comment form.

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Implementation Plan Purpose

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the Critical Infrastructure Protection Reliability Standards, CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "that the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

Implementation Plan Scope

This implementation plan focuses solely on the implementation of the following standards as they apply to nuclear power plants owners and operators:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

Prerequisite approvals or activities

1. FERC must approve the implementation plan for it to take effect. This FERC approval date is referenced in the implementation table by the label "R", signifying the date the Order takes effect.
2. The specific systems, structures, and components must be identified regarding the regulatory jurisdiction in which it resides in order to determine whether NERC CIP standards must be applied. This scope of systems determination, reflected by the label "S", includes the completion of an executed Memorandum of Understanding between

NERC and the NRC on this and other related issues. The scope of system determination also requires the establishment of the exemption process for excluding certain systems, structures, and components from the scope of NERC CIP standards as provided for in Order 706-B.

3. Certain of the NERC CIP standards can only be implemented with the unit off-line. Therefore, certain requirements are likely outage-dependent and are so identified by the label "RO". These items need to be included in the plant's "checkbook" indicated they are planned and budgeted for as part of the planned outage activities. In this context, the refueling outage refers to the first refueling outage at least 12 months beyond the FERC effective date to provide the time needed to plan and budget the activities.

   Specifically, aspects of CIP-005-1, CIP-007-1, and CIP-008-1 requirements pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 if an outage is required to implement the plans, processes, and protocols. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in the self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in the self-certification report, including the time frame needed for implementation for each unit.

Each of these factors can become the critical path item that determines an appropriate timeline for compliance; therefore, the proposed plan is structured that the timeline for compliance becomes the later of:

- the FERC approval date plus an appropriate number of months;
- the scope of systems determination plus an appropriate number of months; or,
- the refueling outage (if applicable) plus an appropriate number of months (to enable the implementation of certain actions during the outage and the completion of the documentation requirements for the implemented changes thereafter)

List of functions that must comply with this implementation plan[1]

- Nuclear Generator Owners
- Nuclear Generator Operators

[1] Note that the CIP standards apply to many additional functional entities – and there is a separate implementation plan, already approved by FERC and other regulatory authorities, that applies to those other functional entities.

CIP-002-1 — Critical Cyber Asset Identification			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	No	R+12 months
R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	No	R+12 months
R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	No	Later of: • R+18 months, or • S+10 months
R4.	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Approval Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-003-1 — Security Management Controls			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009	No	Later of: • R+18 months, or • S+10 months
R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	No	Later of: • R+18 months, or • S+10 months
R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months
R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	No	Later of: • R+18 months, or • S+10 months
R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Approval Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-004-1 — Personnel and Training			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: Direct communications (e.g., emails, memos, computer based training, etc.); Indirect communications (e.g., posters, intranet, brochures, etc.); Management support and reinforcement (e.g., presentations, meetings, etc.).	No	Later of: • R+18 months, or • S+10 months
R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	No	Later of: • R+18 months, or • S+10 months
R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	No	Later of: • R+18 months, or • S+10 months
R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Approval Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-005-1 — Electronic Security Perimeters

Aspects of requirements of CIP-005-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or

			• RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Approval Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 12 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-006-1 — Physical Security of Critical Cyber Assets			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	No	Later of: • R+18 months, or • S+10 months
R3.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	No	Later of: • R+18 months, or • S+10 months
R4.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	No	Later of: • R+18 months, or • S+10 months
R5.	Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	No	Later of: • R+18 months, or • S+10 months
R6.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Approval Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R7.	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	Possible	Later of: • R+18 months, or • S+10 months, or

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
			• RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Approval Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 12 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-008-1 — Incident Reporting and Response Planning

Aspects of requirements of CIP-008-1 pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Approval Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 12 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-009-1 — Recovery Plans for Critical Cyber Assets			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	No	Later of: • R+18 months, or • S+10 months
R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	No	Later of: • R+18 months, or • S+10 months
R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	No	Later of: • R+18 months, or • S+10 months
R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Approval Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form for the Draft Implementation Plan for Version 1 of the CIP Reliability Standards

Please **DO NOT** use this form to submit comments. Please use the electronic form located at the site below to submit comments on the draft Implementation Plan for Version 1 Critical Infrastructure Protection Reliability Standards — CIP-002-1 through CIP-009-1 for Nuclear Power Plants. The electronic comment form must be completed by **August 14, 2009.** In order to be responsive to the September 15, 2009 filing deadline and as a reflection of the significant involvement of the nuclear community in the development of this proposal, the NERC Standards Committee approved the team to shorten the comment period and pre-ballot review period, and if necessary, offer changes to the proposal based on the comments received before proceeding to ballot.

http://www.nerc.com/filez/standards/Cyber_Security_Order706B_Nuclear_Plant_Implementation_Plan.html

If you have questions please contact Gerry Adamski at gerry.adamski@nerc.net or by telephone at 609-524-0617.

Background Information

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the Critical Infrastructure Protection Reliability Standards, CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "that the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

As a standard's implementation plan is a required element per the Reliability Standards Development Procedure, any new or revised plan must proceed through the stakeholder development process. Thus, many members of the original Version 1 Cyber Security Drafting Team agreed to participate in the development of the implementation plan specific for nuclear power plants, with specific outreach to nuclear power plant owners and operators, to ensure their interests were fairly represented and considered in the proposed implementation plan that is the subject of this comment period.

In its consideration, the team contemplated the use of the updated implementation plan that was produced to accompany Version 2 of the CIP standards recently approved by the NERC Board as a starting point for the discussion. The team also recognized in its deliberation that certain of the CIP requirements may require a unit outage to implement. In the end, the team agreed that the approach presented reflects a reasonable schedule for implementation by the US nuclear power plants that acknowledges that cyber security initiatives have been underway within the nuclear industry for several years as instituted by the Nuclear Regulatory Commission and the Nuclear Energy Institute, the nuclear industry's organization for establishing unified policy on matters affecting its constituency.

As background to this last point, in 2004, the nuclear industry completed development of NEI-04-04 that facilitated the establishment of a comprehensive cyber security program for all digital assets at a nuclear plant site. Endorsed by the NRC in late 2005, the program was implemented by all sites in May, 2008. Development work on an updated program began in 2008, titled NEI-08-09, that is intended to assist nuclear plants in complying with newly established NRC regulation 10 CFR 73.54, issued in March, 2009. All nuclear plants are required to submit a detailed cyber security plan and implementation schedule to the NRC by November 23, 2009 as part of the regulation. In addition, as part of the evaluation of FERC's proposed order of clarification that led to Order No. 706-B, the nuclear industry performed an analysis of the NEI-04-04 program and the NERC CIP standards and identified few differences.

Given this context, the drafting team developed the proposed implementation schedule that it believes is an appropriate timeline for compliance by all US nuclear power plants. The timelines described are predicated upon three key aspects:

1. FERC must approve the implementation plan for it to take effect. This FERC approval date is referenced in the table's "Timeframe to Compliance" column by the label "R".
2. The specific systems, structures, and components must be identified regarding the regulatory jurisdiction in which it resides in order to determine whether NERC CIP standards must be applied. This scope of systems determination, reflected by the label "S" in the table's "Timeframe to Compliance" column, includes the completion of an executed Memorandum of Understanding between NERC and the NRC on this and other related issues. The scope of system determination also requires the establishment of the exemption process for excluding certain systems, structures, and components from the scope of NERC CIP standards as provided for in Order 706-B.
3. Certain of the NERC CIP standards can only be implemented with the unit off-line. Therefore, certain requirements are likely outage-dependent and are so identified by the label "RO" in the table's "Timeframe to Compliance" column. These items need to be included in the plant's "checkbook" indicating they are planned and budgeted for as part of the planned outage activities. In this context, the refueling outage refers to the first refueling outage at least 12 months beyond the FERC approval date to provide the time needed to plan and budget the activities.

   Specifically, aspects of CIP-005-1, CIP-007-1, and CIP-008-1 requirements pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 if an outage is required to

implement the plans, processes, and protocols. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Each of these factors can become the critical path item that determines an appropriate timeline for compliance; therefore, the proposed implementation plan is structured so that the timeline for compliance becomes the later of:

- the FERC approval date plus an appropriate number of months;
- the scope of systems determination plus an appropriate number of months; or,
- the refueling outage (if applicable) plus an appropriate number of months (to enable the implementation of certain actions during the outage and the completion of the documentation requirements for the implemented changes thereafter)

In summary, the team is seeking industry input to the proposed implementation plan through the following series of questions. Please note that proposed implementation timeframes are provided only at the main requirement level and all components of the main requirement are therefore intended for inclusion in the timeline.

1. Does the *structure* of the timeframe for compliance represent a reasonable approach that acknowledges the critical path items that could impact implementation of the CIP requirements?

   Comments:

2. Does the proposed implementation plan generally provide a reasonable timeframe for implementing NERC's CIP Version 1 standards at nuclear power plants?

   Comments:

3. Are there any requirements in CIP-002-1 for which the time frame is not suitable for implementation, either not enough time or too much time, to ensure there is no reliability gap in coverage for the balance of plant items at the nuclear power plants in the United States?

   Comments:

4. Are there any requirements in CIP-003-1, CIP-004-1, CIP-006-1, and CIP-009-1 for which the time frame is not suitable for implementation, either not enough time or too much time, to ensure there is no reliability gap in coverage for the balance of plant items at the nuclear power plants in the United States? Implementation of these standards is not believed to be predicated on an outage.

   Comments:

5. Are there any requirements in CIP-005-1, CIP-007-1, and CIP-008-1 for which the time frame is not suitable for implementation, either not enough time or too much time, to ensure there is no reliability gap in coverage for the balance of plant items at the

nuclear power plants in the United States? Implementation of certain aspects of these standards is believed to be predicated on an outage.

Comments:

Individual or group. (15 Responses)
Name (8 Responses)
Organization (8 Responses)
Group Name (7 Responses)
Lead Contact (7 Responses)
Question 1 Comments (15 Responses)
Question 2 Comments (15 Responses)
Question 3 Comments (15 Responses)
Question 4 Comments (15 Responses)
Question 5 Comments (15 Responses)

Group
Exelon Generation Company, LLC - Exelon Nuclear
Alison Mackellar
The structure of the timeframe for compliance presents a generally reasonable approach; however, given that the nuclear industry has not yet performed an assessment in accordance with CIP-002 (R.2, R.3) the scope is difficult to determine.
The proposed implementation plan generally provides a reasonable timeframe for implementing NERC's CIP Version 1 except as noted in the response to other questions, below. In addition, it is our understanding that "Auditably Compliant" will be required one year following the compliance milestone defined in the implementation plan. "Auditably Compliant" means the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable "data," "documents," "documentation," "logs," and "records."
The proposed time frame is suitable for implementation; however, the execution of the identification of a critical asset and identification of critical cyber assets will present a challenge especially during the later milestones that include final review and signoff from senior executives.
For CIP-003-1, CIP-006-1, and CIP-009-1, No. For CIP-004-1, the proposed time frame is reasonable; however, depending on the identified personnel within scope, completion of the training program (R.2) may be a challenge to have completed by the later of the R+18 or S+10 timeframes.
No. The time frames for the requirements in CIP-005-1, CIP-007-1, and CIP-008-1 are suitable for implementation.
Group
Southern Company
Hugh Francis
Yes, the structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. While the structure is accurate there are a few clarifications that need to be made to the structure. While the definition of the "S – Scope of Systems Determination" timeframe includes a statement that the exemption process is included it is not clear if it includes time to file for the exemption. Southern Company would like to ensure the "S" timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the "S" time clock starts. Is the "S" timeframe intended to allow for the exemption process to be complete before the clock starts?
With the exception of the above comment, concerning the "S" timeframe, the items that do not require a refueling outage to implement the timeframes are reasonable for implementing the CIP requirements. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements each unit will first need to be evaluated

against the CIP-002 requirements and be identified as a critical asset. Compliance with this activity is required 12 months after FERC effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified a design change will need to be developed, planned and budgeted to be included into the next refueling outage. With the current implementation schedule each unit would be required to be compliant the latter of R+18, S+10, or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget for the changes, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant then the total time required would be 24 months. In this scenario the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation. In order to allow for adequate time to identify, plan, budget, and implement the required design changes, the definition of RO should be: “RO=Next refueling outage beyond 18 months of FERC Effective Date”

With the exception of the comment to question 1 the time frames are suitable.

With the exception of the comment to question 1 the time frames are suitable. While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.

With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details. While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.

Individual

Doug Engraf

Black & Veatch - Consulting Engineers

We are concerned the time frame between the plant determining the SSCs that are subject to FERC jurisdiction with Memo of Understanding between NERC and NRC and the time to acceptance of that memo. In other words, we are concerned that NERC or the NRC might not accept the SSCs as submitted and the plant's work plan may need significant changes. We would like to see the time to completion tied to acceptance of the SSC list by the NRC and NERC.

The time frame is acceptable as long as long as it is tied to the agreement on which SSCs require NERC CIP compliance.

should not be a problem

With regard to CIP-009-1, deployment of some types of backup and restore systems (including development of complete system backups of CCA's), might be best performed during an outage to prevent impact traffic to ESP network.

Refer to response to Question #1 - If the timeframe is not tied to the NRC and NERC acceptance of the SSC list, the schedule for deployement of the required network security systems, including potential upgrades to existing systems, may be of concern.

Group

PPL Supply Group

Annette Bannon

The structure of the timeframe is reasonable. It reflects the critical path items for the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. The "S" designation is not clear that it includes time to file for an exemption. PPL would like to ensure that the S timeframe allow time for the entity to review the requirements, file for an exemption, and receive a response on the outcome before the S timeclock starts.

PPL does not feel the timeframe allowed for outage activities will provide enough time for identifying solutions, planning, and implementing the requirements. The order of compliance

within 12 months is too short considering once each unit is identified as a critical asset, the critical asset changes budgeted and designed, and then planning and implementing the changes via the work management system. The current implementation schedule is determined as the latter of R+18, S+10, or RO+6. This becomes apparent when an outage would begin 13-14 months after FERC approval. This would require a plant to be compliant in 19-20 months. When we add up all of the design, plan, implement timeframes utilizing our process this would take 24 months...in this case we would have to be compliant in 7-10 months. Therefore the definition of RO needs to change to next refueling outage beyond 18 months of the FERC effective date.

With the exception of the comment to question 1, the time frames are acceptable.

With the exception of the comment to question 1, the time frames are acceptable.

With the exception of the items that require an outage to implement, the timeframes are acceptable. For the items that require an outage to perform, the timeframes are not acceptable, see answer to question 2 above. Consideration needs to be given in these CIPs for the possibility of having to fully implement them in an outage and depends upon the strategy implemented under CIP-005-1.

Individual

Janardan Amin

Luminant Power- CPNPP

Yes, the structure represents a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. While the structure is accurate there are a few clarifications that need to be made to the associated timeframes. While the definition of the “S – Scope of Systems Determination” timeframe includes a statement that the exemption process is included it is not clear if it includes time to file for the exemption. Luminant Power would like to ensure the “S” timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the “S” time clock starts. Is the “S” timeframe intended to allow for the exemption process to be complete before the clock starts?

With the exception of the above comment, concerning the “S” timeframe, the items that do not require a refueling outage to implement, the timeframes are reasonable for implementing the CIP requirements. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements each unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activity is required 12 months after FERC effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified, a design change will need to be developed, planned and budgeted to be included into the next refueling outage. With the current implementation schedule each unit would be required to be compliant the latter of R+18, S+10, or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget for the changes, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant then the total time required would be 24 months. In this scenario the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation. In order to allow for adequate time to identify, plan, budget, and implement the required design changes, the definition of RO should be: “RO=Next refueling outage beyond 18 months of FERC Effective Date”

With the exception of the comment to question 1 the time frames are suitable.

For CIP-003-1, CIP-004-1: With the exception of the comment to question 1 the time frames are suitable. For CIP-006-1: While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process For CIP-009-1: While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement can not be met until that design is implemented. This is also true for

R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.

For CIP-005-1:The time frames allowed for implementing these requirements are not suitable. See answer to question 2 above for details. For CIP-007-1 & CIP-008-1: With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details.

Individual

Marcus Lotto - on behalf of SCE's subject matter experts

Southern California Edison Company

Yes, the structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. While the structure is accurate there are a few clarifications that need to be made to the structure. While the definition of the "S – Scope of Systems Determination" timeframe includes a statement that the exemption process is included it is not clear if it includes time to file for the exemption. Southern California Edison would like to ensure the "S" time frame allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the "S" time clock starts. Is the "S" timeframe intended to allow for the exemption process to be complete before the clock starts? One other item that should be taken into consideration is that the proposed timeline identified in the implementation plan is contingent, in part, on the development of the Memorandum of Understanding (MOU) between NERC and NRC. Because the MOU is intended to address both the "exception process" and audit responsibilities, SCE is concerned with the lack of transparency in MOU development. SCE believes stakeholders would have valuable input into the MOU development, input that would ultimately benefit the industry. Therefore, SCE strongly recommends the MOU development include direct stakeholder participation, or at minimum, solicitation of stakeholder comment prior to adoption.

With the exception of the above comment, concerning the "S" timeframe, the items that do not require a refueling outage to implement the timeframes are reasonable for implementing the CIP requirements. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements each unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activity is required 12 months after FERC effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified a design change will need to be developed, planned and budgeted to be included into the next refueling outage. With the current implementation schedule each unit would be required to be compliant the latter of R+18, S+10, or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget for the changes, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant then the total time required would be 24 months. In this scenario the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation. In order to allow for adequate time to identify, plan, budget, and implement the required design changes, the definition of RO should be: "RO=Next refueling outage beyond 18 months of FERC Effective Date"

With the exception of the comment to question 1, the time frames are suitable.

With the exception of the comment to question 1 the time frames are suitable. While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005, then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.

With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details. While these requirements do not require an

outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance, R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005, then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.
Group
Electric Market Policy
Jalal Babik
The structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. While the structure is adequate, there are a few clarifications that need to be made to the structure. While the definition of the “S – Scope of Stems Determination” timeframe includes a statement that the exemption process is included, it is not clear if it includes time to file for the exemption. Dominion would like to ensure the “S” timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the “S” time clock starts. Is the “S” timeframe intended to allow for the exemption process to be complete before the clock starts?
With the exception of the above comment, concerning the “S” timeframe, the timeframes are reasonable for implementing CIP requirements for the items that do not require a refueling outage to implement. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements, each unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activitiy is required 12 months after the FERC effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified, a design change will need to be developed, planned and budgeted to be included in the next refueling outage. With the current implementation schedule, each unit would be required to be compliant the latter of R+18, S+10 or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant, then the total time required would be 24 months. In this scenario, the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation. In order to allow for adequate time to identify, plan, budget and implement the required design changes, the definition of RO should be: “RO=Next refueling outage beyond 18 months of FERC effective date.”
With the exception of the comment to Question 1, the time frames are suitable.
With the exception of the comment to Question 1, the time frames are suitable. While these requirements do not require an outage to implement, they are dependent on the strategy implemented under CIP-005. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design change to install the access controls per CIP-005, then this requirement cannot be met until the design change is implemented. This is also true for R5 and R6. The Outage dependent column for these requirements (R4, R5 and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self-certification process.
With the exception of the items that require an outage to perform, the time frames are not acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See response to Question 2 above for details. While these requirements do not require an outage to implement, they are dependent on the strategy implemented under CIP-005. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design change to install the access controls per CIP-005, then this requirement cannot be met until the design change is implemented. This is also true for R5 and R6. The Outage dependent column for these requirements (R4, R5 and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self-certification process.
Group

Northeast Power Coordinating Council
Guy Zito
The structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. While the structure is adequate, there are a few clarifications that need to be made to it. While the definition of the “S – Scope of Stems Determination” timeframe includes a statement that the exemption process is included, it is not clear if it includes time to file for the exemption. It should be ensured that the “S” timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the “S” time clock starts. Is the “S” timeframe intended to allow for the exemption process to be complete before the clock starts?
With the exception of the above comment concerning the “S” timeframe, the timeframes are reasonable for implementing CIP requirements for the items that do not require a refueling outage to implement. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements, each unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activitiy is required 12 months after the FERC effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified, a design change will need to be developed, planned and budgeted to be included in the next refueling outage. With the current implementation schedule, each unit would be required to be compliant the latter of R+18, S+10 or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant, then the total time required would be 24 months. In this scenario, the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation. In order to allow for adequate time to identify, plan, budget and implement the required design changes, the definition of RO should be: “RO=Next refueling outage beyond 18 months of FERC effective date.”
With the exception of the comment to Question 1, the timeframes are suitable.
With the exception of the comment to Question 1, the timeframes are suitable. While these requirements do not require an outage to implement, they are dependent on the strategy implemented under CIP-005. For instance, R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design change to install the access controls per CIP-005, then this requirement cannot be met until the design change is implemented. This is also true for R5 and R6. The Outage dependent column for these requirements (R4, R5 and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self-certification process.
With the exception of the items that require an outage to perform, the time frames are not acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See response to Question 2 above for details. While these requirements do not require an outage to implement, they are dependent on the strategy implemented under CIP-005. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design change to install the access controls per CIP-005, then this requirement cannot be met until the design change is implemented. This is also true for R5 and R6. The Outage dependent column for these requirements (R4, R5 and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self-certification process.
Individual
James Starling
SCE&G
Yes, the structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. While the structure is accurate there are a few clarifications that need to be made to the structure. While the definition of the “S – Scope of Systems Determination” timeframe includes a statement that the exemption process is included it is not clear if it includes time to file for the exemption. South Carolina

Electric & Gas would like to ensure the “S” timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the “S” time clock starts. Is the “S” timeframe intended to allow for the exemption process to be complete before the clock starts?
With the exception of the previous comment, concerning the “S” timeframe, the items that do not require a refueling outage to implement the timeframes are reasonable for implementing the CIP requirements. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements the unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activity is required 12 months after FERC effective date. Once the unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified a design change will need to be developed, planned and budgeted to be included into the next refueling outage. With the current implementation schedule each unit would be required to be compliant the latter of R+18, S+10, or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget for the changes, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant then the total time required would be 24 months. In this scenario the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation. In order to allow for adequate time to identify, plan, budget, and implement the required design changes, the definition of RO should be: “RO=Next refueling outage beyond 18 months of FERC Effective Date”
With the exception of the comment to question 1 the time frames are suitable.
CIP-003-1: With the exception of the comment to question 1 the time frames are suitable. CIP-004-1: With the exception of the comment to question 1 the time frames are suitable. CIP-006-1: While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement cannot be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process. CIP-009-1: While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement cannot be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.
CIP-005-1: The time frames allowed for implementing these requirements are not suitable. See answer to question 2 above for details. CIP-007-1: With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details. CIP-008-1: With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details.
Individual
Benjamin Church
NextEra Energy Resources, LLC
Yes, in general the basic structure provides a foundation to establish the correct schedule to implement the reliability standards. One area of concern is in the detail of "S - Scope of Systems Determination" date. There is uncertainty as to whether the MOU between NERC and the NRC will include a matrix or other methodology that will clearly define standard plant systems assigned to NERC or the NRC (i.e., identify the “bright line”). Determination of the "bright line" can also be accomplished by including a period for nuclear plants to evaluate the exemption process, file for exemptions, and receive rulings on filed exemptions. This approach should allow adequate time completion of the exception process before declaring the "S" date.
The prerequisite approvals or activities do not allow for adequate time to implement a compliant program as follows: 1) Nuclear plants will need 12 months to identify assets and any mitigation items that will be required for compliance to CIP-002. Also, there may be plant design changes

required in support of the program requirements. Industry standard "fast track" design changes take 9 months to complete which includes completing the detailed design and establishing complete configuration documentation. Implementation of the engineering design takes an additional 3 months to prepare instructions and complete the work which must be coordinated within the plant work management process. This requires R+24 to perform implementation. 2) Comments from question 1 above identifies the adjustment to "S". 3) Design changes that require a refueling outage impact generation or the safe operation of the plant. Refueling Outages are budgeted, engineered, and planned with longer lead times due to the complexity of work activities. The proposed implementation plan will require some facilities to execute design change packages without adequate time to meet the refueling planning window of 24 months. Adding the 24 months for the refueling design and planning window implementation to the previously stated 12 months for the completion of CIP-002 requires a refueling outage 36 months from the effective date. Some plants have longer fuel cycles so it is recommended the RO effective date is "First refueling outage beyond R +18 month+ one fuel cycle".
See comments from question 1 and 2 above for time frame comments. Implementation of the CIP standards on some Balance of Plant systems is focused on regulatory compliance and the alignment of processes. Due to compliance with NEI 04-04, the industry has implemented cyber security barriers that protect generation and there is no cyber security or reliability gap.
See comments from question 1 and 2 above for time frame comments. Until detailed assessments are completed, it is generally unknown if there are items that can not be installed without a design change during a refueling outage to fully meet all requirements in CIP R03,R04, R06, and R09. The plant should be able to assess the need for a refueling outage to completely satisfy the requirements and provide final reporting during the self certification process. See comments from question 3 above for comments on no reliability gap.
See comments from question 1 and 2 above for time frame comments. See comments from question 3 above for comments on no reliability gap.
Group
Generator Operator
Silvia Parada-Mitchell
Yes, in general the basic structure provides a foundation to establish the correct schedule to implement the reliability standards. One area of concern is in the detail of "S - Scope of Systems Determination" date. There is uncertainty as to whether the MOU between NERC and the NRC will include a matrix or other methodology that will clearly define standard plant systems assigned to NERC or the NRC (i.e., identify the “bright line”). Determination of the "bright line" can also be accomplished by including a period for nuclear plants to evaluate the exemption process, file for exemptions, and receive rulings on filed exemptions. This approach should allow adequate time completion of the exception process before declaring the "S" date.
The prerequisite approvals or activities do not allow for adequate time to implement a compliant program as follows: 1) Nuclear plants will need 12 months to identify assets and any mitigation items that will be required for compliance to CIP-002. Also, there may be plant design changes required in support of the program requirements. Industry standard "fast track" design changes take 9 months to complete which includes completing the detailed design and establishing complete configuration documentation. Implementation of the engineering design takes an additional 3 months to prepare instructions and complete the work which must be coordinated within the plant work management process. This requires R+24 to perform implementation. 2) Comments from question 1 above identifies the adjustment to "S". 3) Design changes that require a refueling outage impact generation or the safe operation of the plant. Refueling Outages are budgeted, engineered, and planned with longer lead times due to the complexity of work activities. The proposed implementation plan will require some facilities to execute design change packages without adequate time to meet the refueling planning window of 24 months. Adding the 24 months for the refueling design and planning window implementation to the previously stated 12 months for the completion of CIP-002 requires a refueling outage 36 months from the effective date. Some plants have longer fuel cycles so it is recommended the RO effective date is "First refueling outage beyond R +18 month+ one fuel cycle".
See comments from question 1 and 2 above for time frame comments. Implementation of the CIP standards on some Balance of Plant systems is focused on regulatory compliance and the alignment of processes. Due to compliance with NEI 04-04, the industry has implemented cyber security barriers that protect generation and there is no cyber security or reliability gap.
See comments from question 1 and 2 above for time frame comments. Until detailed assessments are completed, it is generally unknown if there are items that can not be installed without a design change during a refueling outage to fully meet all requirements in CIP R03,R04, R06, and R09. The plant should be able to assess the need for a refueling outage to completely satisfy the requirements and provide final reporting during the self certification process. See comments from question 3 above for comments on no reliability gap.
See comments from question 1 and 2 above for time frame comments. See comments from question 3 above for comments on no reliability gap.

Individual
Greg Rowland
Duke Energy
Overall, the structure represents a reasonable approach. However, as described in the implementation plan, the “S” (Scope of Systems Determination) seems to include only completion of the NERC/NRC MOU and establishment of the exemption process. 10 months following “S” is barely adequate time for an entity to review the Scope of Systems Determination, identify exemptions and seek NERC approval of the exemptions. NERC will then need time to process exemption requests. NERC’s denial of an exemption should be the event which starts the clock on the “S+10” month timeframe for compliance. That point of denial by NERC would place the item “in scope” and the clock for implementation of CIP standards for that item would start. “S+10” would mean that 10 months after denial of the exemption by NERC you would have to be in compliance. Also, defining “RO” as the first refueling outage 12 months after the FERC effective date does not allow adequate time to design, develop, budget, plan and implement modifications requiring a refueling outage, since some utilities are on a 24-month refueling cycle. “RO” should be defined as the first refueling outage greater than 24 months after the FERC effective date. However, in cases where exemptions are sought for items that require a refueling outage and are subsequently denied by NERC, “RO” should be the first refueling outage greater than 24 months after the denial of the exemption by NERC.
Timeframes are suitable, except for our concern as noted in response to Question #1 above.
Timeframes are suitable, except for our concern as noted in response to Question #1 above.
The implementation plan for CIP-006-1 requirements doesn’t include any “RO+6” timeframes. Depending upon how the physical security plan is implemented, some elements of it might require a refueling outage. Otherwise, timeframes are suitable, except for our concern as noted in response to Question #1 above.
In addition to our concern noted in response to Question #1 above, we have a concern with Requirement R3 of CIP-007-1 which requires installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s). There are many cyber security system devices such as relays and programmable logic controllers which cannot accept software patches. NERC’s technical feasibility exception process doesn’t currently allow an exemption for Requirement R3. If such devices will be required to meet R3, then the timeframe for compliance would be significantly longer than “RO+6”. In some cases, CIP-compliant replacement equipment may not even be available for nuclear-grade applications, and we could NEVER achieve compliance. Similarly, Requirement R5.3.2 requires that passwords shall consist of a combination of alpha, numeric, and “special” characters. Commonly used tools, including Active Directory can enforce password parameters such the following: The password contains characters from at least three of the following five categories: (i) English uppercase characters (A - Z); (ii) English lowercase characters (a - z); (iii) Base 10 digits (0 - 9); (iv) Non-alphanumeric (For example: !, $, #, or %); (v) Unicode characters. We are not aware of password products typically available which can guarantee compliance with the requirement that all three of the parameters (alpha, numeric, and “special” characters) listed in the standard be included in passwords. Unless technical feasibility exceptions are allowed for such legacy Account Management systems, the timeframe for compliance could be significantly longer than “R+18”, “S+10” or “RO+6”.
Group
Progress Energy Nuclear Generation
Chris Georgeson
It can be improved by clarifying that the "S - Scope of Systems Determination" timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response regarding the outcome of the exemption before the "S" time clock starts. This allows time for implementation of requirements for items where an exemption request could be denied.
Individual
William Guldemond
Pacific Gas and Electric/Diablo Canyon Power Plant
Yes
Yes
No
No
No
Individual
Kirit Shah

Ameren
YES.
YES.
NO.
Yes. CIP-006-1 R1, R2, R3 currently do not allow enough time. These requirements need to be changed to outage dependent. Depending on the physical access control changes or a “six-wall” border change the plant may need to be on outage to make these changes.
No.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments for the Draft Implementation Plan for Version 1 of the CIP Reliability Standards

The Order 706B Nuclear Plant Implementation Team thanks all commenters who submitted comments on the Draft Implementation Plan for Version 1 of the CIP Reliability Standards. The implementation plan was posted for a 25-day public comment period from July 20, 2009 through August 14, 2009. In order to be responsive to the September 15, 2009 filing deadline and as a reflection of the significant involvement of the nuclear community in the development of this proposal, the NERC Standards Committee approved the team to shorten the comment period and pre-ballot review period, and if necessary, offer changes to the proposal based on the comments received before proceeding to ballot.

The stakeholders were asked to provide feedback on the draft implementation plan through a special Electronic Comment Form. There were 15 sets of comments, including comments from more than 40 different people from over 25 companies representing 7 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Cyber_Security_Order706B_Nuclear_Plant_Implementation_Plan.html

Based on stakeholder comments, the drafting team made the following changes to the implementation plan:

- Modified the timeframes related to refueling outages to be six months following the completion of the first refueling outage that is at least 18 months following the FERC Effective Date
- Added CIP-006-1 to the list of standards possibly associated with a refueling outage.
- Clarified that the "FERC approval" date is the "FERC approved effective date"

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Hugh Francis	Southern Company	X		X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Neal	Southern Nuclear	SERC	5

2.	Group	Annette Bannon	PPL Supply Group					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Heimbach	PPL Supply	RFC	6
2.	Bill DeLuca	PPL Susquehanna	RFC	5
3.	Dave Gladey	PPL Susquehanna	RFC	5

3.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ralph Rufrano	New York Power Authority	NPCC	5
2.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
3.	Gregory Campoli	New York Independent System Operator	NPCC	2

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10
4.	Roger Champagne	Hydro-Quebec TransEnergie	NPCC	2								
5.	Kurtis Chong	Independent Electricity System Operator	NPCC	2								
6.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1								
7.	Manuel Couto	National Grid	NPCC	1								
8.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1								
9.	Brian D. Evans-Mongeon	Utility Services	NPCC	8								
10.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5								
11.	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC	5								
12.	Kathleen Goodman	ISO - New England	NPCC	2								
13.	David Kiguel	Hydro One Networks Inc.	NPCC	1								
14.	Michael R. Lombardi	Northeast Utilities	NPCC	1								
15.	Randy MacDonald	New Brunswick System Operator	NPCC	2								
16.	Greg Mason	Dynegy Generation	NPCC	5								
17.	Bruce Metruck	New York Power Authority	NPCC	6								
18.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3								
19.	Robert Pellegrini	The United Illuminating Company	NPCC	1								
20.	Michael Schiavone	National Grid	NPCC	1								
21.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10								
22.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10								
4.	Individual	Alison Mackellar	Exelon Generation Company, LLC - Exelon Nuclear					X					
5.	Individual	Doug Engraf	Black & Veatch - Consulting Engineers										
6.	Individual	James Starling	SCE&G	X		X		X	X				
7.	Individual	Benjamin Church	NextEra Energy Resources, LLC					X	X				
8.	Individual	Silvia Parada-Mitchell	Generator Operator	X					X				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
9.	Group	Jalal Babik	Electric Market Policy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jalal Babik		RFC	3
2.	Louis Slade		SERC	6
3.	Mike Garton		NPCC	5
4.	Bill Thompson		SERC	1
5.	Marc Gaudette		SERC	NA

10.	Individual	Chris Georgeson	Progress Energy Nuclear Generation					X					
11.	Individual	Janardan Amin	Luminant Power- CPNPP					X					
12.	Individual	Marcus Lotto - on behalf of SCE's subject matter experts	Southern California Edison Company	X		X		X	X				
13.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
14.	Individual	William Guldemond	Pacific Gas and Electric/Diablo Canyon Power Plant					X					
15.	Individual	Kirit Shah	Ameren	X		X		X	X				

1. Does the *structure* of the timeframe for compliance represent a reasonable approach that acknowledges the critical path items that could impact implementation of the CIP requirements?

Summary Consideration: Commenters generally indicated support for the timeframes but were not clear whether the Scope of Systems Determination included the time to request and receive a response to the exemption request. The team believes the Scope of Systems Determination includes the availability of the exemption process but not the invocation of the process.

Organization	Question 1 Comment
Southern Company	Yes, the structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. While the structure is accurate there are a few clarifications that need to be made to the structure. While the definition of the "S "Scope of Systems Determination? timeframe includes a statement that the exemption process is included it is not clear if it includes time to file for the exemption. Southern Company would like to ensure the "S" timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the "S" time clock starts. Is the "S" timeframe intended to allow for the exemption process to be complete before the clock starts?

Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant.

The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific.

Organization	Question 1 Comment
PPL Supply Group	The structure of the timeframe is reasonable. It reflects the critical path items for the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. The "S" designation is not clear that it includes time to file for an exemption. PPL would like to ensure that the S timeframe allow time for the entity to review the requirements, file for an exemption, and receive a response on the outcome before the S time clock starts.
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific.	
Northeast Power Coordinating Council	The structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. While the structure is adequate, there are a few clarifications that need to be made to it. While the definition of the "S "Scope of Stems Determination? timeframe includes a statement that the exemption process is included, it is not clear if it includes time to file for the exemption. It should be ensured that the "S" timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the "S" time clock starts. Is the "S" timeframe intended to allow for the exemption process to be complete before the clock starts?
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that	

Organization	Question 1 Comment
would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Mermorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific.	
Exelon Generation Company, LLC - Exelon Nuclear	The structure of the timeframe for compliance presents a generally reasonable approach; however, given that the nuclear industry has not yet performed an assessment in accordance with CIP-002 (R.2, R.3) the scope is difficult to determine.
Response: The team thanks you for your comments.	
Black & Veatch - Consulting Engineers	We are concerned the time frame between the plant determining the SSCs that are subject to FERC jurisdiction with Memo of Understanding between NERC and NRC and the time to acceptance of that memo. In other words, we are concerned that NERC or the NRC might not accept the SSCs as submitted and the plant's work plan may need significant changes. We would like to see the time to completion tied to acceptance of the SSC list by the NRC and NERC.
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling	

Organization	Question 1 Comment
outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific.	
SCE&G	Yes, the structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements. While the structure is accurate there are a few clarifications that need to be made to the structure. While the definition of the “S “ Scope of Systems Determination? timeframe includes a statement that the exemption process is included it is not clear if it includes time to file for the exemption. South Carolina Electric & Gas would like to ensure the “S” timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the “S” time clock starts. Is the “S” timeframe intended to allow for the exemption process to be complete before the clock starts?
Response: The reference to the scope of system determination, identified by “S” in the “Timeframe to Compliance” column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC’s CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that	

Organization	Question 1 Comment
contain multiple units as the linkage to refueling outages is unit-specific.	
NextEra Energy Resources, LLC	Yes, in general the basic structure provides a foundation to establish the correct schedule to implement the reliability standards. One area of concern is in the detail of "S - Scope of Systems Determination" date. There is uncertainty as to whether the MOU between NERC and the NRC will include a matrix or other methodology that will clearly define standard plant systems assigned to NERC or the NRC (i.e., identify the "bright line"). Determination of the "bright line" can also be accomplished by including a period for nuclear plants to evaluate the exemption process, file for exemptions, and receive rulings on filed exemptions. This approach should allow adequate time completion of the exception process before declaring the "S" date.
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific.	
Generator Operator	Yes, in general the basic structure provides a foundation to establish the correct schedule to implement the reliability standards. One area of concern is in the detail of "S - Scope of Systems Determination" date. There is uncertainty as to whether the MOU between NERC and the NRC will include a matrix or other methodology that will clearly define standard plant systems assigned to NERC or the NRC (i.e., identify the "bright line"). Determination of the "bright line" can also be accomplished by including a period for nuclear plants to evaluate the exemption process, file for exemptions, and receive rulings on filed exemptions. This approach should allow adequate time completion of the exception process before declaring the "S" date.

Organization	Question 1 Comment
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific.	
Electric Market Policy	The structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements.While the structure is adequate, there are a few clarifications that need to be made to the structure. While the definition of the "S " Scope of Stems Determination? timeframe includes a statement that the exemption process is included, it is not clear if it includes time to file for the exemption.Dominion would like to ensure the "S" timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the "S" time clock starts. Is the "S" timeframe intended to allow for the exemption process to be complete before the clock starts?
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling	

Organization	Question 1 Comment
outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific.	
Progress Energy Nuclear Generation	It can be improved by clarifying that the "S - Scope of Systems Determination" timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response regarding the outcome of the exemption before the "S" time clock starts. This allows time for implementation of requirements for items where an exemption request could be denied.
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific.	
Luminant Power-CPNPP	Yes, the structure represents a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the

Organization	Question 1 Comment
	requirements.While the structure is accurate there are a few clarifications that need to be made to the associated timeframes. While the definition of the "S " Scope of Systems Determination timeframe includes a statement that the exemption process is included it is not clear if it includes time to file for the exemption. Luminant Power would like to ensure the "S" timeframe allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the "S" time clock starts. Is the "S" timeframe intended to allow for the exemption process to be complete before the clock starts?
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific.	
Southern California Edison Company	Yes, the structure of the timeframe is a reasonable approach for the implementation of the CIP requirements at the nuclear plants. The implementation plan accurately reflects the critical path items for the development of the MOU between NERC and the NRC and it also recognizes that a refueling outage is required to implement a portion of the requirements.While the structure is accurate there are a few clarifications that need to be made to the structure. While the definition of the "S " Scope of Systems Determination? timeframe includes a statement that the exemption process is included it is not clear if it includes time to file for the exemption.Southern California Edison would like to ensure the "S" time frame allows time for the entity to review the requirements, file for an exemption, and receive a response on the outcome of the exemption before the "S" time clock starts. Is the "S" timeframe intended to allow for the exemption process to be complete before the clock starts?One other item that should be taken into consideration is that the proposed timeline identified in the implementation plan is contingent, in part, on the development of the Memorandum of Understanding (MOU) between NERC and NRC. Because the MOU is intended to address both the

Organization	Question 1 Comment
	"exception process" and audit responsibilities, SCE is concerned with the lack of transparency in MOU development. SCE believes stakeholders would have valuable input into the MOU development, input that would ultimately benefit the industry. Therefore, SCE strongly recommends the MOU development include direct stakeholder participation, or at minimum, solicitation of stakeholder comment prior to adoption.
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific. The NERC-NRC Memorandum of Understanding is outside the scope of the implementation plan activity that is the subject of this comment period. We will forward your comments to those at NERC working to develop the MOU.	
Duke Energy	Overall, the structure represents a reasonable approach. However, as described in the implementation plan, the "S" (Scope of Systems Determination) seems to include only completion of the NERC/NRC MOU and establishment of the exemption process. 10 months following "S" is barely adequate time for an entity to review the Scope of Systems Determination, identify exemptions and seek NERC approval of the exemptions. NERC will then need time to process exemption requests. NERC's denial of an exemption should be the event which starts the clock on the "S+10" month timeframe for compliance. That point of denial by NERC would place the item "in scope" and the clock for implementation of CIP standards for that item would start. "S+10" would mean that 10 months after denial of the exemption by NERC you would have to be in compliance. Also, defining "RO" as the first refueling outage 12 months after the FERC effective date does not allow adequate time to design, develop, budget, plan and implement modifications requiring a refueling outage, since some utilities are on a 24-month refueling cycle. "RO" should be defined as the first refueling outage greater than 24 months after the FERC effective date. However, in cases where

Organization	Question 1 Comment
	exemptions are sought for items that require a refueling outage and are subsequently denied by NERC, "RO" should be the first refueling outage greater than 24 months after the denial of the exemption by NERC.
Response: The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memoraundum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The actual invocation of the exemption process is not included in this timeframe. However, NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. The amended implementation plan includes three timeframes. The first pertains to requirements not tied to the need for a refueling outage. In these cases, the implementation timeframe is the FERC effective date plus 18 months. For those requirements that are outage-dependent, the timeframe to compliance is six months following the first refueling outage at least 18 months from the FERC Effective Date. And the final component is the scope of systems determination for which the timeframe to compliance is ten months following the completion of the Memorandum of Understanding and the estalbishment of the exemption process. The controlling timeframe for implementation is the later of the three. As the completion of the Memorandum of Understanding and the availability of the exemption process is expected in the next few months, the controlling timeframe is expected to be the FERC Effective Date plus 18 months. Given that each nuclear power plant is required to file a comprehensive cyber security plan with the NRC in November, 2009, the team believes sufficient time exists for an entity to invoke and receive disposition of the request for exemption before the NERC CIP standards take effect. To be clear, the implementation timeframes for CIP requirements are intended to be applied on a per unit basis for those plants that contain multiple units as the linkage to refueling outages is unit-specific. The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	
Pacific Gas and Electric/Diablo Canyon Power Plant	Yes
Ameren	YES.

2. Does the proposed implementation plan generally provide a reasonable timeframe for implementing NERC's CIP Version 1 standards at nuclear power plants?

Summary Consideration: Commenters expressed concern that the timeframes associated with a refueling outage may not be sufficient to fully design and implement changes in support of the CIP standards. The team agreed and modified the timeframes related to refueling outages to be six months following the completion of the first refueling outage that is at least 18 months following the FERC Effective Date.

Organization	Question 2 Comment
Southern Company	With the exception of the above comment, concerning the "S" timeframe, the items that do not require a refueling outage to implement the timeframes are reasonable for implementing the CIP requirements. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements each unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activity is required 12 months after FERC effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified a design change will need to be developed, planned and budgeted to be included into the next refueling outage. With the current implementation schedule each unit would be required to be compliant the latter of R+18, S+10, or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget for the changes, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant then the total time required would be 24 months. In this scenario the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation. In order to allow for adequate time to identify, plan, budget, and implement the required design changes, the definition of RO should be: RO=Next refueling outage beyond 18 months of FERC Effective Date?

Response: The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the

Organization	Question 2 Comment
refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	
PPL Supply Group	PPL does not feel the timeframe allowed for outage activities will provide enough time for identifying solutions, planning, and implementing the requirements. The order of compliance within 12 months is too short considering once each unit is identified as a critical asset, the critical asset changes budgeted and designed, and then planning and implementing the changes via the work management system. The current implementation schedule is determined as the latter of R+18, S+10, or RO+6. This becomes apparent when an outage would begin 13-14 months after FERC approval. This would require a plant to be compliant in 19-20 months. When we add up all of the design, plan, implement timeframes utilizing our process this would take 24 months...in this case we would have to be compliant in 7-10 months. Therefore the definition of RO needs to change to next refueling outage beyond 18 months of the FERC effective date.
Response: The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	
Northeast Power Coordinating Council	With the exception of the above comment concerning the “S” timeframe, the timeframes are reasonable for implementing CIP requirements for the items that do not require a refueling outage to implement. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements, each unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activitiy is required 12 months after the FERC effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified, a design change will need to be developed, planned and budgeted to be included in the next refueling outage.With the current implementation schedule, each unit would be required to be compliant the latter of R+18, S+10 or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is

Organization	Question 2 Comment
	complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant, then the total time required would be 24 months. In this scenario, the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation.In order to allow for adequate time to identify, plan, budget and implement the required design changes, the definition of RO should be: RO=Next refueling outage beyond 18 months of FERC effective date.?
Response: The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	
Exelon Generation Company, LLC - Exelon Nuclear	The proposed implementation plan generally provides a reasonable timeframe for implementing NERC's CIP Version 1 except as noted in the response to other questions, below.In addition, it is our understanding that "Auditably Compliant" will be required one year following the compliance milestone defined in the implementation plan. "Auditably Compliant" means the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable "data," "documents," "documentation," "logs," and "records."
Response: The team agrees with your description of "Auditably Compliant"	
Black & Veatch - Consulting Engineers	The time frame is acceptable as long as long as it is tied to the agreement on which SSCs require NERC CIP compliance.
Response: Agreed.	
SCE&G	With the exception of the previous comment, concerning the "S" timeframe, the items that do not require a refueling outage to implement the timeframes are reasonable for implementing the CIP requirements. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements the unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activity is required 12 months after FERC effective date. Once the unit is identified as a critical asset, the critical cyber assets will need to be identified. Once

Organization	Question 2 Comment
	the critical cyber assets are identified a design change will need to be developed, planned and budgeted to be included into the next refueling outage. With the current implementation schedule each unit would be required to be compliant the latter of R+18, S+10, or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget for the changes, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant then the total time required would be 24 months. In this scenario the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation. In order to allow for adequate time to identify, plan, budget, and implement the required design changes, the definition of RO should be: RO=Next refueling outage beyond 18 months of FERC Effective Date?
Response: The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	
NextEra Energy Resources, LLC	The prerequisite approvals or activities do not allow for adequate time to implement a compliant program as follows: 1) Nuclear plants will need 12 months to identify assets and any mitigation items that will be required for compliance to CIP-002. Also, there may be plant design changes required in support of the program requirements. Industry standard "fast track" design changes take 9 months to complete which includes completing the detailed design and establishing complete configuration documentation. Implementation of the engineering design takes an additional 3 months to prepare instructions and complete the work which must be coordinated within the plant work management process. This requires R+24 to perform implementation. 2) Comments from question 1 above identifies the adjustment to "S". 3) Design changes that require a refueling outage impact generation or the safe operation of the plant. Refueling Outages are budgeted, engineered, and planned with longer lead times due to the complexity of work activities. The proposed implementation plan will require some facilities to execute design change packages without adequate time to meet the refueling planning window of 24 months. Adding the 24 months for the refueling design and planning window implementation to the previously stated 12 months for the completion of CIP-002 requires a refueling outage 36 months from the effective date. Some plants have longer fuel cycles so it is

Organization	Question 2 Comment
	recommended the RO effective date is "First refueling outage beyond R +18 month+ one fuel cycle".
Response: The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	
Generator Operator	The prerequisite approvals or activities do not allow for adequate time to implement a compliant program as follows: 1) Nuclear plants will need 12 months to identify assets and any mitigation items that will be required for compliance to CIP-002. Also, there may be plant design changes required in support of the program requirements. Industry standard "fast track" design changes take 9 months to complete which includes completing the detailed design and establishing complete configuration documentation. Implementation of the engineering design takes an additional 3 months to prepare instructions and complete the work which must be coordinated within the plant work management process. This requires R+24 to perform implementation. 2) Comments from question 1 above identifies the adjustment to "S". 3) Design changes that require a refueling outage impact generation or the safe operation of the plant. Refueling Outages are budgeted, engineered, and planned with longer lead times due to the complexity of work activities. The proposed implementation plan will require some facilities to execute design change packages without adequate time to meet the refueling planning window of 24 months. Adding the 24 months for the refueling design and planning window implementation to the previously stated 12 months for the completion of CIP-002 requires a refueling outage 36 months from the effective date. Some plants have longer fuel cycles so it is recommended the RO effective date is "First refueling outage beyond R +18 month+ one fuel cycle".
Response: The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	

Organization	Question 2 Comment
Electric Market Policy	With the exception of the above comment, concerning the "S" timeframe, the timeframes are reasonable for implementing CIP requirements for the items that do not require a refueling outage to implement. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements, each unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activitiy is required 12 months after the FERC effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified, a design change will need to be developed, planned and budgeted to be included in the next refueling outage.With the current implementation schedule, each unit would be required to be compliant the latter of R+18, S+10 or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant, then the total time required would be 24 months. In this scenario, the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation.In order to allow for adequate time to identify, plan, budget and implement the required design changes, the definition of RO should be: RO=Next refueling outage beyond 18 months of FERC effective date.?
Response: The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	
Luminant Power-CPNPP	With the exception of the above comment, concerning the "S" timeframe, the items that do not require a refueling outage to implement, the timeframes are reasonable for implementing the CIP requirements. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements each unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activity is required 12 months after FERC

Organization	Question 2 Comment
	effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified, a design change will need to be developed, planned and budgeted to be included into the next refueling outage. With the current implementation schedule each unit would be required to be compliant the latter of R+18, S+10, or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to effectively plan and budget for the changes, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant then the total time required would be 24 months. In this scenario the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation. In order to allow for adequate time to identify, plan, budget, and implement the required design changes, the definition of RO should be: RO=Next refueling outage beyond 18 months of FERC Effective Date?
Response: The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	
Southern California Edison Company	With the exception of the above comment, concerning the “S” timeframe, the items that do not require a refueling outage to implement the timeframes are reasonable for implementing the CIP requirements. However, we do not feel the timeframe allowed for outage activities will provide enough time for identification, planning and implementing the requirements. The current plan provides a timeframe for outage activities of the first refueling outage 12 months after FERC approval. In order to comply with the requirements each unit will first need to be evaluated against the CIP-002 requirements and be identified as a critical asset. Compliance with this activity is required 12 months after FERC effective date. Once each unit is identified as a critical asset, the critical cyber assets will need to be identified. Once the critical cyber assets are identified a design change will need to be developed, planned and budgeted to be included into the next refueling outage.With the current implementation schedule each unit would be required to be compliant the latter of R+18, S+10, or RO+6. The worst case scenario is if an outage is scheduled to begin 13-14 months after FERC approval. The current timeframe would require the unit to have a plan, including design change, approval of the budget, implemented and documentation updated in 19-20 months to be compliant. In order to

Organization	Question 2 Comment
	effectively plan and budget for the changes, we would first need to develop a design change. A design change of this type would take a minimum of 6 months. Once the development of the design change is complete we could accurately plan and budget for the change. This will take an additional 6 months. If the identification requires 12 months to be compliant then the total time required would be 24 months. In this scenario the plant is allowed approximately 7-10 months, after identifying it as a critical asset, to develop a design change, plan, implement and update the documentation.In order to allow for adequate time to identify, plan, budget, and implement the required design changes, the definition of RO should be: RO=Next refueling outage beyond 18 months of FERC Effective Date?
Response: The team agrees that the part of the implementation plan linked to refueling outages is confusing relative to other apsects of the implementation plan, particularly in the timeframe 12-18 months following the FERC Effective Date. Therefore, for simplicity and to recognize that the controlling timeframe will be at least 18 months following the FERC Effective Date, the team has modified the implementation timeframes for those requirements linked to refueling outages to be six months following the first refueling outage that is at least 18 months from the FERC Effective Date. The team believes this approach simplifies the plan by targeting implementation for those requirements not tied to an outage at 18 months following the FERC Effective Date, or for those requirements that are outage-related, at six months following the first refueling outage that is at least 18 months following the FERC Effective Date. The six months identified for the refueling outage permits the entity to complete the necessary documentation for the modification or activities that were undertaken during the outage.	
Duke Energy	Timeframes are suitable, except for our concern as noted in response to Question #1 above.
Response: Thank you for your comment	
Pacific Gas and Electric/Diablo Canyon Power Plant	Yes
Ameren	YES.

3. Are there any requirements in CIP-002-1 for which the time frame is not suitable for implementation, either not enough time or too much time, to ensure there is no reliability gap in coverage for the balance of plant items at the nuclear power plants in the United States?

Summary Consideration: Commenters indicated that except as identified in earlier questions, the timeframes are suitable.

Organization	Question 3 Comment
Southern Company	With the exception of the comment to question 1 the time frames are suitable.
PPL Supply Group	With the exception of the comment to question 1, the time frames are acceptable.
Response: Thank you for your comment	
Northeast Power Coordinating Council	With the exception of the comment to Question 1, the timeframes are suitable.
Response: Thank you for your comment	
Exelon Generation Company, LLC - Exelon Nuclear	The proposed time frame is suitable for implementation; however, the execution of the identification of a critical asset and identification of critical cyber assets will present a challenge especially during the later milestones that include final review and signoff from senior executives.
Response: Thank you for your comment	
Black & Veatch - Consulting Engineers	should not be a problem
Response: Thank you for your comment	
SCE&G	With the exception of the comment to question 1 the time frames are suitable.
Response: Thank you for your comment	
NextEra Energy	See comments from question 1 and 2 above for time frame comments. Implementation of the CIP standards on some Balance

Organization	Question 3 Comment
Resources, LLC	of Plant systems is focused on regulatory compliance and the alignment of processes. Due to compliance with NEI 04-04, the industry has implemented cyber security barriers that protect generation and there is no cyber security or reliability gap.
Response: Thank you for your comment	
Generator Operator	See comments from question 1 and 2 above for time frame comments. Implementation of the CIP standards on some Balance of Plant systems is focused on regulatory compliance and the alignment of processes. Due to compliance with NEI 04-04, the industry has implemented cyber security barriers that protect generation and there is no cyber security or reliability gap.
Response: Thank you for your comment	
Electric Market Policy	With the exception of the comment to Question 1, the time frames are suitable.
Response: Thank you for your comment	
Progress Energy Nuclear Generation	
Luminant Power- CPNPP	With the exception of the comment to question 1 the time frames are suitable.
Southern California Edison Company	With the exception of the comment to question 1, the time frames are suitable.
Response: Thank you for your comment	
Duke Energy	Timeframes are suitable, except for our concern as noted in response to Question #1 above.
Response: Thank you for your comment	
Pacific Gas and Electric/Diablo Canyon Power Plant	No
Ameren	NO.

4. Are there any requirements in CIP-003-1, CIP-004-1, CIP-006-1, and CIP-009-1 for which the time frame is not suitable for implementation, either not enough time or too much time, to ensure there is no reliability gap in coverage for the balance of plant items at the nuclear power plants in the United States? Implementation of these standards is not believed to be predicated on an outage.

Summary Consideration: Several commenters indicated concern over CIP-006-1 not being available for implementation except during a refueling outage timeframe. The team agreed and included CIP-006-1 on the list of standards possibly associated with a refueling outage. Other commenters indicated that all standards should have their implementation plan linked to refueling outages. The team does not believe this is appropriate and that non-outage related approaches are available to meet the intent of the remaining requirements.

Organization	Question 4 Comment
Southern Company	With the exception of the comment to question 1 the time frames are suitable.While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement. However, the team does not agree that CIP-003-1, CIP-004-1, and CIP-009-1 should be linked to a refueling outage. The team believes that there are interim solutions that could be implemented manually if necessary to meet the intent of the requirements. The entity could then determine the appropriateness of installing more permanent and perhaps automated solutions during the next refueling outage opportunity.	
PPL Supply Group	With the exception of the comment to question 1, the time frames are acceptable.
Response: Thank you for your comment.	
Northeast Power Coordinating Council	With the exception of the comment to Question 1, the timeframes are suitable. While these requirements do not require an outage to implement, they are dependent on the strategy implemented under CIP-005. For instance, R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design change to install the access controls per CIP-005, then this requirement cannot be met until the design change is implemented. This is also true for R5 and R6. The Outage dependent column for these requirements (R4, R5 and R6) should be labeled as Possible and the RO+6 timeframe

Organization	Question 4 Comment
	should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self-certification process.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement. However, the team does not agree that CIP-003-1, CIP-004-1, and CIP-009-1 should be linked to a refueling outage. The team believes that there are interim solutions that could be implemented manually if necessary to meet the intent of the requirements. The entity could then determine the appropriateness of installing more permanent and perhaps automated solutions during the next refueling outage opportunity.	
Exelon Generation Company, LLC - Exelon Nuclear	For CIP-003-1, CIP-006-1, and CIP-009-1, No. For CIP-004-1, the proposed time frame is reasonable; however, depending on the identified personnel within scope, completion of the training program (R.2) may be a challenge to have completed by the later of the R+18 or S+10 timeframes.
Response: The team does not agree with the suggestion to modify the implementation timeframes for training program requirements in CIP-004-1. The entity's training program can include provisions to exclude personnel who have not completed the training program with the understanding that the person would not have access or be included on access lists for CCAs prior to the training being completed.	
Black & Veatch - Consulting Engineers	With regard to CIP-009-1, deployment of some types of backup and restore systems (including development of complete system backups of CCA's), might be best performed during an outage to prevent impact traffic to ESP network.
Response: The team appreciates the comment but believes CIP-009-1 is appropriately classified. As the language in the requirement states, Requirement R4 requires the development of the process and procedures for backup and restore; it does not require a technical control that would require an outage to implement. Further, the team believes the implementation of those processes and procedures could be performed manually and would also not require an outage	
SCE&G	CIP-003-1: With the exception of the comment to question 1 the time frames are suitable. CIP-004-1: With the exception of the comment to question 1 the time frames are suitable. CIP-006-1: While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement cannot be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process. CIP-009-1: While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement cannot be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6)

Organization	Question 4 Comment
	should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement. However, the team does not agree that CIP-003-1, CIP-004-1, and CIP-009-1 should be linked to a refueling outage. The team believes that there are interim solutions that could be implemented manually if necessary to meet the intent of the requirements. The entity could then determine the appropriateness of installing more permanent, and perhaps automated solutions during the next refueling outage opportunity	
NextEra Energy Resources, LLC	See comments from question 1 and 2 above for time frame comments. Until detailed assessments are completed, it is generally unknown if there are items that can not be installed without a design change during a refueling outage to fully meet all requirements in CIP R03,R04, R06, and R09. The plant should be able to assess the need for a refueling outage to completely satisfy the requirements and provide final reporting during the self certification process.See comments from question 3 above for comments on no reliability gap.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement. However, the team does not agree that CIP-003-1, CIP-004-1, and CIP-009-1 should be linked to a refueling outage. The team believes that there are interim solutions that could be implemented manually if necessary to meet the intent of the requirements. The entity could then determine the appropriateness of installing more permanent, and perhaps automated solutions during the next refueling outage opportunity	
Generator Operator	See comments from question 1 and 2 above for time frame comments. Until detailed assessments are completed, it is generally unknown if there are items that can not be installed without a design change during a refueling outage to fully meet all requirements in CIP R03,R04, R06, and R09. The plant should be able to assess the need for a refueling outage to completely satisfy the requirements and provide final reporting during the self certification process.See comments from question 3 above for comments on no reliability gap.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement. However, the team does not agree that CIP-003-1, CIP-004-1, and CIP-009-1 should be linked to a refueling outage. The team believes that there are interim solutions that could be implemented manually if necessary to meet the intent of the requirements. The entity could then determine the appropriateness of installing more permanent, and perhaps automated solutions during the next refueling outage opportunity	
Electric Market Policy	With the exception of the comment to Question 1, the time frames are suitable. While these requirements do not require an outage to implement, they are dependent on the strategy implemented under CIP-005. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design change to install the access controls per

Organization	Question 4 Comment
	CIP-005, then this requirement cannot be met until the design change is implemented. This is also true for R5 and R6. The Outage dependent column for these requirements (R4, R5 and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self-certification process.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement. However, the team does not agree that CIP-003-1, CIP-004-1, and CIP-009-1 should be linked to a refueling outage. The team believes that there are interim solutions that could be implemented manually if necessary to meet the intent of the requirements. The entity could then determine the appropriateness of installing more permanent, and perhaps automated solutions during the next refueling outage opportunity	
Progress Energy Nuclear Generation	
Luminant Power-CPNPP	For CIP-003-1, CIP-004-1: With the exception of the comment to question 1 the time frames are suitable.For CIP-006-1: While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification processFor CIP-009-1: While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement. However, the team does not agree that CIP-003-1, CIP-004-1, and CIP-009-1 should be linked to a refueling outage. The team believes that there are interim solutions that could be implemented manually if necessary to meet the intent of the requirements. The entity could then determine the appropriateness of installing more permanent, and perhaps automated solutions during the next refueling outage opportunity	
Southern California Edison Company	With the exception of the comment to question 1 the time frames are suitable.While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-

Organization	Question 4 Comment
	005, then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement. However, the team does not agree that CIP-003-1, CIP-004-1, and CIP-009-1 should be linked to a refueling outage. The team believes that there are interim solutions that could be implemented manually if necessary to meet the intent of the requirements. The entity could then determine the appropriateness of installing more permanent, and perhaps automated solutions during the next refueling outage opportunity	
Duke Energy	The implementation plan for CIP-006-1 requirements doesn't include any "RO+6" timeframes. Depending upon how the physical security plan is implemented, some elements of it might require a refueling outage. Otherwise, timeframes are suitable, except for our concern as noted in response to Question #1 above.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement.	
Pacific Gas and Electric/Diablo Canyon Power Plant	No
Ameren	Yes. CIP-006-1 R1, R2, R3 currently do not allow enough time. These requirements need to be changed to outage dependent. Depending on the physical access control changes or a "six-wall" border change the plant may need to be on outage to make these changes.
Response: The team has re-evaluated CIP-006-1 and modified the implementation plan to include CIP-006-1 in the list of standards that could potentially require an outage to implement. The implementation of physical controls, particularly outside the protected area, could require an outage to fully implement.	

5. Are there any requirements in CIP-005-1, CIP-007-1, and CIP-008-1 for which the time frame is not suitable for implementation, either not enough time or too much time, to ensure there is no reliability gap in coverage for the balance of plant items at the nuclear power plants in the United States? Implementation of certain aspects of these standards is believed to be predicated on an outage.

Summary Consideration: No concern expressed with respect to these standards except for the time concerns addressed earlier regarding refueling outages.

Organization	Question 5 Comment
Southern Company	With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details.While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005 then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.
Response: See responses to earlier questions.	
PPL Supply Group	With the exception of the items that require an outage to implement, the timeframes are acceptable. For the items that require an outage to perform, the timeframes are not acceptable, see answer to question 2 above. Consideration needs to be given in these CIPs for the possibility of having to fully implement them in an outage and depends upon the strategy implemented under CIP-005-1.
Response: See responses to earlier questions	
Northeast Power Coordinating Council	With the exception of the items that require an outage to perform, the time frames are not acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See response to Question 2 above for details.While these requirements do not require an outage to implement, they are dependent on the strategy implemented under CIP-005. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design change to install the access controls per CIP-005, then this requirement cannot be met until the design change is implemented. This is also true for R5 and R6. The Outage dependent column for these requirements (R4, R5 and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self-certification process.

Organization	Question 5 Comment
Response: See responses to earlier questions	
Exelon Generation Company, LLC - Exelon Nuclear	No. The time frames for the requirements in CIP-005-1, CIP-007-1, and CIP-008-1 are suitable for implementation.
Response: See responses to earlier questions	
Black & Veatch - Consulting Engineers	Refer to response to Question #1 - If the timeframe is not tied to the NRC and NERC acceptance of the SSC list, the schedule for deployement of the required network security systems, including potential upgrades to existing systems, may be of concern.
Response: See responses to earlier questions	
SCE&G	CIP-005-1: The time frames allowed for implementing these requirements are not suitable. See answer to question 2 above for details. CIP-007-1: With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details. CIP-008-1: With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details.
Response: See responses to earlier questions	
NextEra Energy Resources, LLC	See comments from question 1 and 2 above for time frame comments.See comments from question 3 above for comments on no reliability gap.
Generator Operator	See comments from question 1 and 2 above for time frame comments.See comments from question 3 above for comments on no reliability gap.
Response: See responses to earlier questions	
Electric Market Policy	With the exception of the items that require an outage to perform, the time frames are not acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See response to Question 2 above for details.While these requirements do not require an outage to implement, they are dependent on the strategy implemented under CIP-005. For instance R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design change to install the access controls per CIP-005, then this requirement cannot be met until the design change is

Organization	Question 5 Comment
	implemented. This is also true for R5 and R6. The Outage dependent column for these requirements (R4, R5 and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self-certification process.
Response: See responses to earlier questions	
Progress Energy Nuclear Generation	
Luminant Power-CPNPP	For CIP-005-1:The time frames allowed for implementing these requirements are not suitable. See answer to question 2 above for details.For CIP-007-1 & CIP-008-1: With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details.
Response: See responses to earlier questions	
Southern California Edison Company	With the exception of the items that require an outage to perform, the time frames are acceptable. For the items that require an outage to perform, the time frames allowed are not suitable. See answer to question 2 above for details. While these requirements do not require an outage to implement they are dependent on the strategy implemented under CIP-005-1. For instance, R4 requires the entity to log access 24 hours a day, 7 days a week. If the plant identifies the need for a design to install the access controls per CIP-005, then this requirement can not be met until that design is implemented. This is also true for R5 and R6. The Outage Dependent column for these requirements (R4, R5, and R6) should be labeled as Possible and the RO+6 timeframe should be included. The entity should be able to assess the need for an outage to satisfy these requirements and report that during the self certification process.
Response: See responses to earlier questions	
Duke Energy	In addition to our concern noted in response to Question #1 above, we have a concern with Requirement R3 of CIP-007-1 which requires installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s). There are many cyber security system devices such as relays and programmable logic controllers which cannot accept software patches. NERC's technical feasibility exception process doesn't currently allow an exemption for Requirement R3. If such devices will be required to meet R3, then the timeframe for compliance would be significantly longer than "RO+6". In some cases, CIP-compliant replacement equipment may not even be available for nuclear-grade applications, and we could NEVER achieve compliance.Similarly, Requirement R5.3.2 requires that passwords shall consist of a combination of alpha, numeric, and "special" characters. Commonly used tools, including Active Directory can enforce password parameters such the following: The password contains characters from at least three of the following five

Organization	Question 5 Comment
	categories: (i) English uppercase characters (A - Z); (ii) English lowercase characters (a - z); (iii) Base 10 digits (0 - 9); (iv) Non-alphanumeric (For example: !, $, #, or %); (v) Unicode characters. We are not aware of password products typically available which can guarantee compliance with the requirement that all three of the parameters (alpha, numeric, and "special" characters) listed in the standard be included in passwords. Unless technical feasibility exceptions are allowed for such legacy Account Management systems, the timeframe for compliance could be significantly longer than "R+18", "S+10" or "RO+6".
Response: The existing R3.2 language permits a technical feasibility exception already. This requirement states: *The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk. and permits the entity* Therefore, the team believes the commenter's concern, while valid, is already addressed through R3.2 provisions. Requirement R5.3.2 already is included on the list of requirements for which a technical feasibility exception can be requested.	
Pacific Gas and Electric/Diablo Canyon Power Plant	No
Ameren	No.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Initial Ballot Window Open

August 19–28, 2009

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Cyber Security — Order 706B Nuclear Plant Implementation Plan

An initial ballot window for an implementation plan for Version 1 critical infrastructure protection (CIP) Reliability Standards CIP-002-1 through CIP-009-1 for Nuclear Power Plants is now open **until 8 p.m. EDT on August 28, 2009**.

Special Notes for This Project

In order to be responsive to the September 15, 2009 filing deadline and as a reflection of the significant involvement of the nuclear community in the development of this proposal, the NERC Standards Committee approved the team to shorten the comment period and hold the comment period at the same time as the pre-ballot review period, and if necessary, offer changes to the proposal based on the comments received before proceeding to ballot. The comment period and pre-ballot review ended on August 14, 2009. The drafting team modified the implementation plan based on stakeholder input; the two significant revisions are listed below:

1. Included CIP-006-1 on the list of standards potentially requiring an outage to implement
2. Adjusted the implementation timeframe for refueling outages to six months beyond the first refueling outage that is at least 18 months following the FERC effective date

Instructions

Members of the ballot pool associated with this project may log in and submit their votes from the following page: https://standards.nerc.net/CurrentBallots.aspx

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the CIP Reliability Standards: CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

This project addresses the development of the implementation plan specific for nuclear power plants. The draft plan was drafted by members of the original Version 1 Cyber Security Drafting Team with specific outreach to nuclear power plant owners and operators to ensure their interests were fairly represented.

Project page:
http://www.nerc.com/filez/standards/Cyber_Security_Order706B_Nuclear_Plant_Implementation_Plan.html

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Implementation Plan Purpose

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the Critical Infrastructure Protection Reliability Standards, CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "that the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

Implementation Plan Scope

This implementation plan focuses solely on the implementation of the following standards as they apply to nuclear power plants owners and operators:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

Prerequisite approvals or activities

1. FERC must approve the implementation plan for it to take effect. This FERC approved effective date is referenced in the implementation table by the label "R", signifying the date the Order takes effect.
2. The specific systems, structures, and components must be identified regarding the regulatory jurisdiction in which it resides in order to determine whether NERC CIP standards must be applied. This scope of systems determination, reflected by the label "S", includes the completion of an executed Memorandum of Understanding between

NERC and the NRC on this and other related issues. The scope of system determination also requires the establishment of the exemption process for excluding certain systems, structures, and components from the scope of NERC CIP standards as provided for in Order 706-B.

3. Certain of the NERC CIP standards can only be implemented with the unit off-line. Therefore, certain requirements are likely outage-dependent and are so identified by the label "RO". These items need to be included in the plant's "checkbook" indicated they are planned and budgeted for as part of the planned outage activities. In this context, the refueling outage refers to the first refueling outage at least 18 months beyond the FERC effective date to provide the time needed to plan and budget the activities.

   Specifically, aspects of CIP-005-1, CIP-006-1, CIP-007-1, and CIP-008-1 requirements pertaining to the **development** of plans, processes, and protocols shall be completed the later of FERC Effective Date ("R") +18 months or Scope of Systems Determination ("S") +10 months. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or six months following the completion of the first refueling outage at least 18 months following the FERC Effective Date ("RO")if an outage is required to implement the plans, processes, and protocols. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in the self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in the self-certification report, including the time frame needed for implementation for each unit.

Each of these factors can become the critical path item that determines an appropriate timeline for compliance; therefore, the proposed plan is structured that the timeline for compliance becomes the later of:

- the FERC Effective Date plus 18 months;
- the Scope of Systems Determination plus 10 months; or,
- six months following the completion of the first refueling outage (if applicable) at least 18 months following the FERC Effective Date. The added six months enables the entity to complete the documentation requirements for the implemented changes.

List of functions that must comply with this implementation plan[1]

- Nuclear Generator Owners
- Nuclear Generator Operators

[1] Note that the CIP standards apply to many additional functional entities – and there is a separate implementation plan, already approved by FERC and other regulatory authorities, that applies to those other functional entities.

CIP-002-1 — Critical Cyber Asset Identification			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	No	R+12 months
R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	No	R+12 months
R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	No	Later of: • R+18 months, or • S+10 months
R4.	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-003-1 — Security Management Controls			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009	No	Later of: • R+18 months, or • S+10 months
R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	No	Later of: • R+18 months, or • S+10 months
R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months
R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	No	Later of: • R+18 months, or • S+10 months
R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

CIP-004-1 — Personnel and Training			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: Direct communications (e.g., emails, memos, computer based training, etc.); Indirect communications (e.g., posters, intranet, brochures, etc.); Management support and reinforcement (e.g., presentations, meetings, etc.).	No	Later of: • R+18 months, or • S+10 months
R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	No	Later of: • R+18 months, or • S+10 months
R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	No	Later of: • R+18 months, or • S+10 months
R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-005-1 — Electronic Security Perimeters

Aspects of requirements of CIP-005-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-006-1 — Physical Security of Critical Cyber Assets

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	Possible	Later of: • R+18 months, or • S+10 months, or

			• RO+6 months (if applicable)
R6.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Account Management — The Responsible Entity shall establish, implement, and	Possible	Later of:

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
	document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.		• R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R7.	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-008-1 — Incident Reporting and Response Planning

Aspects of requirements of CIP-008-1 pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-009-1 — Recovery Plans for Critical Cyber Assets			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	No	Later of: • R+18 months, or • S+10 months
R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	No	Later of: • R+18 months, or • S+10 months
R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	No	Later of: • R+18 months, or • S+10 months
R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

Implementation Plan Purpose

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the Critical Infrastructure Protection Reliability Standards, CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "that the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

Implementation Plan Scope

This implementation plan focuses solely on the implementation of the following standards as they apply to nuclear power plants owners and operators:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

Prerequisite approvals or activities

1. FERC must approve the implementation plan for it to take effect. This FERC ~~approval~~ approved effective date is referenced in the implementation table by the label "R", signifying the date the Order takes effect.
2. The specific systems, structures, and components must be identified regarding the regulatory jurisdiction in which it resides in order to determine whether NERC CIP standards must be applied. This scope of systems determination, reflected by the label "S", includes the completion of an executed Memorandum of Understanding between

NERC and the NRC on this and other related issues. The scope of system determination also requires the establishment of the exemption process for excluding certain systems, structures, and components from the scope of NERC CIP standards as provided for in Order 706-B.

3. Certain of the NERC CIP standards can only be implemented with the unit off-line. Therefore, certain requirements are likely outage-dependent and are so identified by the label "RO". These items need to be included in the plant's "checkbook" indicated they are planned and budgeted for as part of the planned outage activities. In this context, the refueling outage refers to the first refueling outage at least ~~12~~ 18 months beyond the FERC effective date to provide the time needed to plan and budget the activities.

   Specifically, aspects of CIP-005-1, CIP-006-1, CIP-007-1, and CIP-008-1 requirements pertaining to the **development** of plans, processes, and protocols shall be completed the later of ~~R~~FERC Effective Date ("R") +18 months or Scope of Systems Determination ("S") +10 months.~~-~~ For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or ~~RO~~six months following the completion of the first refueling outage at least 18 months following the FERC Effective Date ("RO")~~+6~~ if an outage is required to implement the plans, processes, and protocols.~~ -~~ The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in the self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in the self-certification report, including the time frame needed for implementation for each unit.

Each of these factors can become the critical path item that determines an appropriate timeline for compliance; therefore, the proposed plan is structured that the timeline for compliance becomes the later of:

- the FERC ~~approval~~ Effective D~~d~~ate plus ~~an appropriate number of~~18 months;
- the S~~s~~cope of ~~systems~~ Systems ~~determination~~ Determination plus ~~an appropriate number of~~10 months; or,
- six months following the completion of the first~~the~~ refueling outage (if applicable) at least 18 months following the FERC Effective Date. The added six months ~~plus an appropriate number of months (to~~ enables the ~~implementation of certain actions during the outage and the~~ entity to complet~~ion of~~e the documentation requirements for the implemented changes~~ thereafter)~~.

List of functions that must comply with this implementation plan[1]

- Nuclear Generator Owners

[1] Note that the CIP standards apply to many additional functional entities – and there is a separate implementation plan, already approved by FERC and other regulatory authorities, that applies to those other functional entities.

- Nuclear Generator Operators

CIP-002-1 — Critical Cyber Asset Identification			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	No	R+12 months
R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	No	R+12 months
R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	No	Later of: • R+18 months, or • S+10 months
R4.	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC ~~Approval~~ Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-003-1 — Security Management Controls			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009	No	Later of: • R+18 months, or • S+10 months
R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	No	Later of: • R+18 months, or • S+10 months
R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months
R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	No	Later of: • R+18 months, or • S+10 months
R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC ~~Approval~~ Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-004-1 — Personnel and Training			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: Direct communications (e.g., emails, memos, computer based training, etc.); Indirect communications (e.g., posters, intranet, brochures, etc.); Management support and reinforcement (e.g., presentations, meetings, etc.).	No	Later of: • R+18 months, or • S+10 months
R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	No	Later of: • R+18 months, or • S+10 months
R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	No	Later of: • R+18 months, or • S+10 months
R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective~~Approval~~ Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

CIP-005-1 — Electronic Security Perimeters

Aspects of requirements of CIP-005-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or

			• RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective~~Approval~~ Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond ~~12~~ 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-006-1 — Physical Security of Critical Cyber Assets

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

R5.	Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R6.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC EffectiveApproval Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R7.	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	Possible	Later of: • R+18 months, or • S+10 months, or

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
			• RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective~~Approval~~ Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond ~~12~~ 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-008-1 — Incident Reporting and Response Planning

Aspects of requirements of CIP-008-1 pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective~~Approval~~ Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond ~~12~~ 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-009-1 — Recovery Plans for Critical Cyber Assets			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	No	Later of: • R+18 months, or • S+10 months
R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	No	Later of: • R+18 months, or • S+10 months
R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	No	Later of: • R+18 months, or • S+10 months
R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective~~Approval~~ Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Initial Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Cyber Security — Order 706B Nuclear Plant Implementation Plan
The initial ballot for an implementation plan for Version 1 critical infrastructure protection (CIP) Reliability Standards CIP-002-1 through CIP-009-1 for Nuclear Power Plants ended on August 28, 2009.

Ballot Results
Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results:

Quorum: 81.96%
Approval: 97.37%

Since at least one negative ballot included a comment, these results are not final. A second (or recirculation) ballot must be conducted. Ballot criteria details are listed at the end of the announcement.

Next Steps
As part of the recirculation ballot process, the drafting team must draft and post responses to voter comments. The drafting team will also determine whether or not to make revisions to the balloted item(s). Should the team decide to make revisions, the revised item(s) will return to the initial ballot phase.

Project Background
On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the CIP Reliability Standards: CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

This project addresses the development of the implementation plan specific for nuclear power plants. The draft plan was drafted by members of the original Version 1 Cyber Security Drafting Team with specific outreach to nuclear power plant owners and operators to ensure their interests were fairly represented.

Project page:
http://www.nerc.com/filez/standards/Cyber_Security_Order706B_Nuclear_Plant_Implementation_Plan.html

Special Notes for This Project

In order to be responsive to the September 15, 2009 filing deadline and as a reflection of the significant involvement of the nuclear community in the development of this proposal, the NERC Standards Committee approved the team to shorten the comment period and hold the comment period at the same time as the pre-ballot review period, and if necessary, offer changes to the proposal based on the comments received before proceeding to ballot. The comment period and pre-ballot review ended on August 14, 2009. The drafting team modified the implementation plan based on stakeholder input; the two significant revisions are listed below:

1. Included CIP-006-1 on the list of standards potentially requiring an outage to implement
2. Adjusted the implementation timeframe for refueling outages to six months beyond the first refueling outage that is at least 18 months following the FERC effective date

Standards Development Process

The *Reliability Standards Development Procedure* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

Ballot Criteria

Approval requires both a (1) quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) A two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses. If there are no negative votes with reasons from the first ballot, the results of the first ballot shall stand. If, however, one or more members submit negative votes with reasons, a second ballot shall be conducted.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Ballot Results	
Ballot Name:	Order 706-B Nuclear Implementation Plan_in
Ballot Period:	8/19/2009 - 8/28/2009
Ballot Type:	Initial
Total # Votes:	159
Total Ballot Pool:	194
Quorum:	**81.96 % The Quorum has been reached**
Weighted Segment Vote:	97.37 %
Ballot Results:	**The standard will proceed to recirculation ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	48	1	31	0.939	2	0.061	6	9
2 - Segment 2.	9	0.3	3	0.3	0	0	2	4
3 - Segment 3.	47	1	30	1	0	0	11	6
4 - Segment 4.	10	0.5	5	0.5	0	0	3	2
5 - Segment 5.	34	1	22	0.957	1	0.043	8	3
6 - Segment 6.	26	1	16	0.941	1	0.059	3	6
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.6	6	0.6	0	0	0	2
9 - Segment 9.	5	0.2	2	0.2	0	0	1	2
10 - Segment 10.	7	0.6	6	0.6	0	0	0	1
Totals	**194**	**6.2**	**121**	**6.037**	**4**	**0.163**	**34**	**35**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	CenterPoint Energy	Paul Rocha	Abstain	
1	Central Maine Power Company	Brian Conroy	Affirmative	

1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba		
1	Entergy Corporation	George R. Bartlett	Affirmative	View
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	Farmington Electric Utility System	Alan Glazner		
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	ITC Transmission	Elizabeth Howell	Affirmative	
1	JEA	Ted E. Hobson	Abstain	
1	Kansas City Power & Light Co.	Michael Gammon		
1	Kissimmee Utility Authority	Joe B Watson	Affirmative	
1	Lakeland Electric	Larry E Watt	Abstain	
1	Lincoln Electric System	Doug Bantam		
1	MEAG Power	Danny Dees	Affirmative	
1	National Grid	Manuel Couto		
1	Nebraska Public Power District	Richard L. Koch	Abstain	
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura		
1	Oncor Electric Delivery	Charles W. Jenkins		
1	Pacific Gas and Electric Company	Chifong L. Thomas	Affirmative	
1	PacifiCorp	Mark Sampson		
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Negative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	SaskPower	Wayne Guttormson	Abstain	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Affirmative	
1	Tri-State G & T Association Inc.	Keith V. Carman	Abstain	
1	Westar Energy	Allen Klassen		
1	Xcel Energy, Inc.	Gregory L. Pieper	Affirmative	
2	Alberta Electric System Operator	Anita Lee		
2	BC Transmission Corporation	Faramarz Amjadi	Abstain	
2	California ISO	Greg Tillitson		
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Abstain	
2	New Brunswick System Operator	Alden Briggs		
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Affirmative	
3	Alabama Power Company	Bobby Kerley	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City Public Service of San Antonio	Edwin Les Barrow		
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	David A. Lapinski	Abstain	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Affirmative	View
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	

3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	Edward W Pourciau	Abstain	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen		
3	Gulf Power Company	Gwen S Frazier	Affirmative	
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker	Abstain	
3	Kansas City Power & Light Co.	Charles Locke		
3	Lincoln Electric System	Bruce Merrill	Abstain	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Abstain	
3	Mississippi Power	Don Horsley	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Abstain	
3	New York Power Authority	Michael Lupo	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters	Abstain	
3	PacifiCorp	John Apperson	Abstain	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	View
3	Public Utility District No. 2 of Grant County	Greg Lange		
3	Sacramento Municipal Utility District	Mark Alberter	Abstain	
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson		
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin L Holt		
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Northern California Power Agency	Fred E. Young	Abstain	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R. Wallace		
4	Wisconsin Energy Corp.	Anthony Jankowski	Abstain	
5	AEP Service Corp.	Brock Ondayko		
5	Amerenue	Sam Dwyer	Affirmative	
5	Avista Corp.	Edward F. Groce	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Constellation Power Source Generation, Inc.	Scott A Etnoyer	Abstain	
5	Consumers Energy	James B Lewis	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	View
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	FPL Energy	Benjamin Church	Negative	
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	JEA	Donald Gilbert	Abstain	
5	Kansas City Power & Light Co.	Scott Heidtbrink		
5	Lincoln Electric System	Dennis Florom		
5	Louisville Gas and Electric Co.	Charlie Martin	Abstain	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Abstain	
5	Northern States Power Co.	Liam Noailles	Affirmative	
5	Orlando Utilities Commission	Richard Kinas	Abstain	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp Energy	David Godfrey	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Abstain	
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	

5	PSEG Power LLC	Thomas Piascik	Affirmative	View
5	Salt River Project	Glen Reeves	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	South Carolina Electric & Gas Co.	Richard Jones	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	View
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Negative	View
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Thomas Saitta		
6	Lincoln Electric System	Eric Ruskamp	Abstain	
6	Louisville Gas and Electric Co.	Daryn Barker	Abstain	
6	Luminant Energy	Thomas Burke		
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Abstain	
6	PacifiCorp	Gregory D Maxfield	Affirmative	
6	PP&L, Inc.	Thomas Hyzinski	Affirmative	
6	Progress Energy	James Eckelkamp	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Southern California Edison Co.	Marcus V Lotto	Affirmative	
6	Tampa Electric Co.	Joann Wehle		
6	Western Area Power Administration - UGP Marketing	John Stonebarger		
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8	Edward C Stein	Edward C Stein	Affirmative	
8	James A Maenner	James A Maenner	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Roger C Zaklukiewicz	Roger C Zaklukiewicz	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
8	Wally Magda	Wally Magda	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	Maine Public Utilities Commission	Jacob A McDermott	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G Dvorsky		
9	Public Utilities Commission of Ohio	Klaus Lambeck		
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Affirmative	
10	Midwest Reliability Organization	Dan R Schoenecker	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Jacquie Smith	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren		

Account Log-In/Register

Consideration of Comments on Initial Ballot — Order 706-B Nuclear Implementation Plan

Summary Consideration:

The initial ballot received nine comments from representatives in four of ten segments. The drafting team did not make any modifications to the Order 706B Implementation Plan based on balloter comments. The commenters expressed concerns in the following areas:

- The timeframe for scope of systems determination in the plan (denoted by "S") should include time to request and receive a response to an exemption request. The drafting team addressed this item in the previous comment period and concluded the invocation of the process is not included in this timeframe.
- The timeframe for requirements related to a refueling outage is insufficient and needs to be modified to be 6 months following the first outage that is at least 18 months following the FERC effective date. The team had previously made this change prior to initiating the ballot.
- CIP-006 and CIP-007 requirements need to be identified as possibly needing a refueling outage to implement. The team had previously made this change prior to initiating the ballot.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Voter	Entity	Segment	Vote	Comment
Silvia P Mitchell	Florida Power & Light Co.	6	Negative	Although partial clarification was provided to S (Scope of System Determination) and to implementation timeframes, additional consideration should be given to nuclear power plants for the development and implementation of a cyber security program that is fully compliant to the NERC CIP Reliability Standards. This additional consideration would involve a more thorough vetting of the exemption process and of the implementation timeframes that support design changes and nuclear refueling outage planning windows. The implementation timeframe is crucial for allowing adequate time to develop/implement design changes, develop/implement procedural instructions, and develop/implement proper training elements for the nuclear operators who already maintain a rigorous training schedule.

[1] The appeals process is in the Reliability Standards Development Procedure: http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memorandum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The exemption process will contain the procedural details and a reasonable timeline to dispose of the requests as NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. However, the actual invocation of the exemption process is not included in this timeframe. Overall, the drafting team feels the proposed implementation plan respects the time needed by the nuclear power plant owners and operators to properly implement the NERC CIP standards, including specific accommodations for activities dependent on outages to implement.				
George R. Bartlett Matt Wolf Terri F Benoit Stanley M Jaskot	Entergy Corporation Entergy Services, Inc. Entergy Corporation	1 3 6 5	Affirmative	1. For CIP-002-1, CIP-003-1, CIP-004-1, CIP-006-1 and CIP-009-1, the Scope of Systems Determination (S) timeframe needs to allow additional up-front time for requesting an exemption and getting a decision on the request prior to the "S + 10 months" implementation period taking effect. If this were factored into the S timeframe, the structure of the timeframe for compliance would represent a reasonable approach that would acknowledge the critical path items which could impact implementation of the CIP requirements. 2. There is insufficient time allotted after the FERC effective date to get outage required activities fully scoped and planned. The existing definition of RO (Next Refueling Outage beyond 12 months of FERC Effective Date) should be changed to equal the next refueling outage beyond 18 months after the FERC effective date. 3. For CIP-006-1 under Requirements 4, 5 and 6, the Outage Dependent column needs to be changed from "No" to "Possible" with a RO+6 months (if applicable) timeframe. 4. For CIP-007-1 under Requirements 4 and 6, the Outage Dependent column needs to be changed from "No" to "Possible" with a RO+6 months (if applicable) timeframe.
Response: 1. Thank you for your comments. The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memorandum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The exemption process will contain the procedural details and a reasonable timeline to dispose of the requests as NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations				

Voter	Entity	Segment	Vote	Comment
				and to maximize the time to become compliant. However, the actual invocation of the exemption process is not included in this timeframe. 2. In response to comments received during the industry posting of the implementation plan prior to the balloting phase, the drafting team changed the timeframe associated with a refueling outage to that suggested – RO+6 months where RO is the first refueling outage at least 18 months following the FERC effective date. Therefore, the plan ballotted already reflects this change. 3. The suggested change was made in response to comments received during the industry comment period that preceded the ballot. Therefore, the plan ballotted already reflects this change. 4. The suggested change was made in response to comments received during the industry comment period that preceded the ballot. Therefore, the plan ballotted already reflects this change.
Jeffrey Mueller Thomas Piascik James D. Hebson	Public Service Electric and Gas Co. PSEG Power LLC PSEG Energy Resources & Trade LLC	3 5 6	Affirmative	1. PSEG believes that the structure of the timeframe is reasonable, and in the interests of moving forward is voting in favor. However, PSEG requests that the "S" timeframe be clarified to state that it is intended to allow sufficient time for the entity to review the requirements, file for an exemption and receive a response on the outcome of the exemption before the "S" time clock starts. 2. Also, PSEG does not believe that as presently written in some cases the timeframe allowed for outage activities will provide sufficient time to identify, plan and implement the CIP requirements including required design changes. Thus the definition of "RO" should be specified as the first refueling outage commencing 18 months after the FERC effective date.
Response: 1. Thank you for your comments. The reference to the scope of system determination, identified by "S" in the "Timeframe to Compliance" column, includes the time necessary to complete (1) the NERC-NRC Memorandum of Understanding; and, (2) the development of the exemption process that would permit entities to request exclusion of certain systems, structures, and components from the scope of NERC's CIP standards. The Memorandum of Understanding, to be completed in the next few months, is expected to contain a clear delineation of the systems, structures, and components under NRC and NERC jurisdiction. The exemption process will contain the procedural details and a reasonable timeline to dispose of the requests as NERC understands the need to process exemption requests efficiently to ensure entities are clear on expectations and to maximize the time to become compliant. However, the actual invocation of the exemption process is not included in this timeframe.				

Voter	Entity	Segment	Vote	Comment
2. In response to comments received during the industry posting of the implementation plan prior to the balloting phase, the drafting team changed the timeframe associated with a refueling outage to that suggested – RO+6 months where RO is the first refueling outage at least 18 months following the FERC effective date. Therefore, the plan ballotted already reflects this change.				
Nickesha P Carrol	Consolidated Edison Co. of New York	6	Affirmative	Regarding the CIP-005 question which is on R4.2.2: we would prefer clarification to the last sentence “Devices controlling access into the Electronic Security Perimeter are not exempt.” Suggest removing or replacing with “Devices controlling access into the Electronic Security Perimeter must comply with the Standards, as described in CIP-005 R1.5.”.
Response: Thank you for your comment. The issue raised relates to a change in the language of the standard itself and is outside the scope of this team’s activities that is solely focused on the implementation plan.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Recirculation Ballot Window Open
September 1–10, 2009

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Cyber Security — Order 706B Nuclear Plant Implementation Plan

A recirculation ballot window for an implementation plan for Version 1 critical infrastructure protection (CIP) Reliability Standards CIP-002-1 through CIP-009-1 for Nuclear Power Plants is now open **until 8 p.m. EDT on September 10, 2009**.

Instructions

Members of the ballot pool associated with this project may log in and submit their votes from the following page: https://standards.nerc.net/CurrentBallots.aspx

Recirculation Ballot Process

The Standards Committee encourages all members of the ballot pool to review the consideration of comments submitted with the initial ballots. In the recirculation ballot, votes are counted by exception only — if a ballot pool member does not submit a revision to that member's original vote, the vote remains the same as in the first ballot. Members of the ballot pool may:

- Reconsider and change their vote from the first ballot.
- Vote in the second ballot even if they did not vote on the first ballot.
- Take no action if they do not want to change their original vote.

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the CIP Reliability Standards: CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.

> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

This project addresses the development of the implementation plan specific for nuclear power plants. The draft plan was drafted by members of the original Version 1 Cyber Security Drafting Team with specific outreach to nuclear power plant owners and operators to ensure their interests were fairly represented.

Project page:
http://www.nerc.com/filez/standards/Cyber_Security_Order706B_Nuclear_Plant_Implementation_Plan.html

Special Notes for This Project

In order to be responsive to the September 15, 2009 filing deadline and as a reflection of the significant involvement of the nuclear community in the development of this proposal, the NERC Standards Committee approved the team to shorten the comment period and hold the comment period at the same time as the pre-ballot review period, and if necessary, offer changes to the proposal based on the comments received before proceeding to ballot. The comment period and pre-ballot review ended on August 14, 2009. The drafting team modified the implementation plan based on stakeholder input; the two significant revisions are listed below:

1. Included CIP-006-1 on the list of standards potentially requiring an outage to implement
2. Adjusted the implementation timeframe for refueling outages to six months beyond the first refueling outage that is at least 18 months following the FERC effective date

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Implementation Plan Purpose

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the Critical Infrastructure Protection Reliability Standards, CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "that the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

Implementation Plan Scope

This implementation plan focuses solely on the implementation of the following standards as they apply to nuclear power plants owners and operators:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

Prerequisite approvals or activities

1. FERC must approve the implementation plan for it to take effect. This FERC approved effective date is referenced in the implementation table by the label "R", signifying the date the Order takes effect.
2. The specific systems, structures, and components must be identified regarding the regulatory jurisdiction in which it resides in order to determine whether NERC CIP standards must be applied. This scope of systems determination, reflected by the label "S", includes the completion of an executed Memorandum of Understanding between

NERC and the NRC on this and other related issues. The scope of system determination also requires the establishment of the exemption process for excluding certain systems, structures, and components from the scope of NERC CIP standards as provided for in Order 706-B.

3. Certain of the NERC CIP standards can only be implemented with the unit off-line. Therefore, certain requirements are likely outage-dependent and are so identified by the label "RO". These items need to be included in the plant's "checkbook" indicated they are planned and budgeted for as part of the planned outage activities. In this context, the refueling outage refers to the first refueling outage at least 18 months beyond the FERC effective date to provide the time needed to plan and budget the activities.

   Specifically, aspects of CIP-005-1, CIP-006-1, CIP-007-1, and CIP-008-1 requirements pertaining to the **development** of plans, processes, and protocols shall be completed the later of FERC Effective Date ("R") +18 months or Scope of Systems Determination ("S") +10 months. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or six months following the completion of the first refueling outage at least 18 months following the FERC Effective Date ("RO")if an outage is required to implement the plans, processes, and protocols. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in the self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in the self-certification report, including the time frame needed for implementation for each unit.

Each of these factors can become the critical path item that determines an appropriate timeline for compliance; therefore, the proposed plan is structured that the timeline for compliance becomes the later of:

- the FERC Effective Date plus 18 months;
- the Scope of Systems Determination plus 10 months; or,
- six months following the completion of the first refueling outage (if applicable) at least 18 months following the FERC Effective Date. The added six months enables the entity to complete the documentation requirements for the implemented changes.

List of functions that must comply with this implementation plan[1]

- Nuclear Generator Owners
- Nuclear Generator Operators

[1] Note that the CIP standards apply to many additional functional entities – and there is a separate implementation plan, already approved by FERC and other regulatory authorities, that applies to those other functional entities.

CIP-002-1 — Critical Cyber Asset Identification			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	No	R+12 months
R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	No	R+12 months
R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	No	Later of: • R+18 months, or • S+10 months
R4.	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-003-1 — Security Management Controls			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009	No	Later of: • R+18 months, or • S+10 months
R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	No	Later of: • R+18 months, or • S+10 months
R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months
R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	No	Later of: • R+18 months, or • S+10 months
R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

CIP-004-1 — Personnel and Training			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: Direct communications (e.g., emails, memos, computer based training, etc.); Indirect communications (e.g., posters, intranet, brochures, etc.); Management support and reinforcement (e.g., presentations, meetings, etc.).	No	Later of: • R+18 months, or • S+10 months
R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	No	Later of: • R+18 months, or • S+10 months
R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	No	Later of: • R+18 months, or • S+10 months
R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-005-1 — Electronic Security Perimeters

Aspects of requirements of CIP-005-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-006-1 — Physical Security of Critical Cyber Assets

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	Possible	Later of: • R+18 months, or • S+10 months, or

			• RO+6 months (if applicable)
R6.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Account Management — The Responsible Entity shall establish, implement, and	Possible	Later of:

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
	document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.		• R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R7.	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-008-1 — Incident Reporting and Response Planning

Aspects of requirements of CIP-008-1 pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-009-1 — Recovery Plans for Critical Cyber Assets			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	No	Later of: • R+18 months, or • S+10 months
R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	No	Later of: • R+18 months, or • S+10 months
R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	No	Later of: • R+18 months, or • S+10 months
R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

Implementation Plan Purpose

On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the Critical Infrastructure Protection Reliability Standards, CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "that the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

Implementation Plan Scope

This implementation plan focuses solely on the implementation of the following standards as they apply to nuclear power plants owners and operators:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

Prerequisite approvals or activities

1. FERC must approve the implementation plan for it to take effect. This FERC ~~approval~~ approved effective date is referenced in the implementation table by the label "R", signifying the date the Order takes effect.
2. The specific systems, structures, and components must be identified regarding the regulatory jurisdiction in which it resides in order to determine whether NERC CIP standards must be applied. This scope of systems determination, reflected by the label "S", includes the completion of an executed Memorandum of Understanding between

NERC and the NRC on this and other related issues. The scope of system determination also requires the establishment of the exemption process for excluding certain systems, structures, and components from the scope of NERC CIP standards as provided for in Order 706-B.

3. Certain of the NERC CIP standards can only be implemented with the unit off-line. Therefore, certain requirements are likely outage-dependent and are so identified by the label "RO". These items need to be included in the plant's "checkbook" indicated they are planned and budgeted for as part of the planned outage activities. In this context, the refueling outage refers to the first refueling outage at least ~~12~~ 18 months beyond the FERC effective date to provide the time needed to plan and budget the activities.

   Specifically, aspects of CIP-005-1, CIP-006-1, CIP-007-1, and CIP-008-1 requirements pertaining to the **development** of plans, processes, and protocols shall be completed the later of ~~R~~FERC Effective Date ("R") +18 months or Scope of Systems Determination ("S") +10 months.~~-~~ For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or ~~RO~~six months following the completion of the first refueling outage at least 18 months following the FERC Effective Date ("RO")~~+6~~ if an outage is required to implement the plans, processes, and protocols.~~ -~~ The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in the self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in the self-certification report, including the time frame needed for implementation for each unit.

Each of these factors can become the critical path item that determines an appropriate timeline for compliance; therefore, the proposed plan is structured that the timeline for compliance becomes the later of:

- the FERC ~~approval~~ Effective D~~d~~ate plus ~~an appropriate number of~~18 months;
- the S~~s~~cope of ~~systems~~ Systems ~~determination~~ Determination plus ~~an appropriate number of~~10 months; or,
- six months following the completion of the first~~the~~ refueling outage (if applicable) at least 18 months following the FERC Effective Date. The added six months ~~plus an appropriate number of months (to~~ enables the ~~implementation of certain actions during the outage and the~~ entity to complet~~ion of~~e the documentation requirements for the implemented changes~~ thereafter)~~.

List of functions that must comply with this implementation plan[1]

- Nuclear Generator Owners

[1] Note that the CIP standards apply to many additional functional entities – and there is a separate implementation plan, already approved by FERC and other regulatory authorities, that applies to those other functional entities.

- Nuclear Generator Operators

CIP-002-1 — Critical Cyber Asset Identification			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	No	R+12 months
R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	No	R+12 months
R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	No	Later of: • R+18 months, or • S+10 months
R4.	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC ~~Approval~~ Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-003-1 — Security Management Controls			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009	No	Later of: • R+18 months, or • S+10 months
R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	No	Later of: • R+18 months, or • S+10 months
R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months
R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	No	Later of: • R+18 months, or • S+10 months
R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	No	Later of: • R+18 months, or • S+10 months

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC ~~Approval~~ Effective Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.

CIP-004-1 — Personnel and Training			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: Direct communications (e.g., emails, memos, computer based training, etc.); Indirect communications (e.g., posters, intranet, brochures, etc.); Management support and reinforcement (e.g., presentations, meetings, etc.).	No	Later of: • R+18 months, or • S+10 months
R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	No	Later of: • R+18 months, or • S+10 months
R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	No	Later of: • R+18 months, or • S+10 months
R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective~~Approval~~ Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

CIP-005-1 — Electronic Security Perimeters

Aspects of requirements of CIP-005-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or

			• RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective~~Approval~~ Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond ~~12~~ 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-006-1 — Physical Security of Critical Cyber Assets

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

R5.	Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R6.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	PossibleNo	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC EffectiveApproval Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R7.	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	Possible	Later of: • R+18 months, or • S+10 months, or

CIP-007-1 — Systems Security Management

Aspects of requirements of CIP-007-1pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
			• RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective~~Approval~~ Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond ~~12~~ 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-008-1 — Incident Reporting and Response Planning

Aspects of requirements of CIP-008-1 pertaining to the **development** of plans, processes, and protocols shall be completed the later of R+18 or S+10. For aspects of requirements that implement the plans, processes, and protocols (and related documentation requirements regarding that implementation), the Responsible Entity shall **perform the implementation** the later of R+18 or S+10 or RO+6 *if an outage is required to implement the plans, processes, and protocols*. The Responsible Entity will be expected to assess whether a refueling outage is needed during the initial self-certification process for the CIP Version 1 standards for nuclear power plants and provide the information in its self-certification report. For multi-unit nuclear power plants, should separate outages be required to implement the plans, processes, ands protocols for all units at the plant, the Responsible Entity shall indicate the need for separate outages in its self-certification report, including the time frame needed for implementation for each unit.

Requirement Number	Text of Requirement	Outage-Dependent	Timeframe to Compliance
R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)
R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	Possible	Later of: • R+18 months, or • S+10 months, or • RO+6 months (if applicable)

Abbreviations in "Timeframe to Compliance" Column:

- R = FERC Effective~~Approval~~ Date.
- S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.
- **RO= Next Refueling Outage beyond ~~12~~ 18 months of FERC Effective Date**; Placed into the 'Plant Checkbook' (planned and budgeted) at the earliest time frame commensurate with the risk of the modification

CIP-009-1 — Recovery Plans for Critical Cyber Assets			
Requirement Number	**Text of Requirement**	**Outage-Dependent**	**Timeframe to Compliance**
R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	No	Later of: • R+18 months, or • S+10 months
R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	No	Later of: • R+18 months, or • S+10 months
R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	No	Later of: • R+18 months, or • S+10 months
R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	No	Later of: • R+18 months, or • S+10 months
R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	No	Later of: • R+18 months, or • S+10 months
Abbreviations in "Timeframe to Compliance" Column: • R = FERC Effective~~Approval~~ Date. • S = Scope of Systems Determination. Scope of Systems Determination includes establishing the FERC and NRC jurisdictional delineation for systems, structures, and components that is predicated upon the completion of a NERC-NRC Memorandum of Understanding, and the Order 706-B exemption process for removing elements from the scope of NERC's CIP standards.			

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Final Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Cyber Security — Order 706B Nuclear Plant Implementation Plan
The recirculation ballot for an implementation plan for Version 1 critical infrastructure protection (CIP) reliability standards CIP-002-1 through CIP-009-1 for nuclear power plants ended September 10, 2009.

Ballot Results
Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results:

Quorum: 87.11%
Approval: 97.18%

The ballot pool approved the implementation plan. Ballot criteria details are listed at the end of the announcement.

Next Steps
The implementation plan will be submitted to the NERC Board of Trustees for adoption.

Project Background
On January 18, 2008, FERC (or "Commission") issued Order No. 706 that approved Version 1 of the CIP standards: CIP-002-1 through CIP-009-1. On March 19, 2009, the Commission issued clarifying Order No. 706-B that clarified "the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706." However, in the ensuing discussion regarding the implementation timeframe for the nuclear power plants to comply with the CIP standards, the Commission noted in ¶59 that,

> "[i]t is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.
>
> Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to

> develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule."

This project addresses the development of the implementation plan specific for nuclear power plants. The draft plan was drafted by members of the original Version 1 Cyber Security Drafting Team with specific outreach to nuclear power plant owners and operators to ensure their interests were fairly represented.

Project page:
http://www.nerc.com/filez/standards/Cyber_Security_Order706B_Nuclear_Plant_Implementation_Plan.html

Standards Development Process

The *Reliability Standards Development Procedure* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

Ballot Criteria

Approval requires both a (1) quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) A two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses. If there are no negative votes with reasons from the first ballot, the results of the first ballot shall stand. If, however, one or more members submit negative votes with reasons, a second ballot shall be conducted.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Ballot Results

Ballot Name:	Order 706-B Nuclear Implementation Plan_rc
Ballot Period:	9/1/2009 - 9/10/2009
Ballot Type:	recirculation
Total # Votes:	169
Total Ballot Pool:	194
Quorum:	**87.11 % The Quorum has been reached**
Weighted Segment Vote:	97.18 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	48	1	32	0.941	2	0.059	7	7
2 - Segment 2.	9	0.4	4	0.4	0	0	2	3
3 - Segment 3.	47	1	31	0.969	1	0.031	11	4
4 - Segment 4.	10	0.6	6	0.6	0	0	3	1
5 - Segment 5.	34	1	22	0.957	1	0.043	8	3
6 - Segment 6.	26	1	18	0.947	1	0.053	3	4
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.7	7	0.7	0	0	0	1
9 - Segment 9.	5	0.2	2	0.2	0	0	1	2
10 - Segment 10.	7	0.7	7	0.7	0	0	0	0
Totals	**194**	**6.6**	**129**	**6.414**	**5**	**0.186**	**35**	**25**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Jason Shaver	Affirmative	
1	BC Transmission Corporation	Gordon Rawlings	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	CenterPoint Energy	Paul Rocha	Abstain	
1	Central Maine Power Company	Brian Conroy	Affirmative	

1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dominion Virginia Power	William L. Thompson	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba		
1	Entergy Corporation	George R. Bartlett	Affirmative	View
1	Exelon Energy	John J. Blazekovich	Affirmative	
1	Farmington Electric Utility System	Alan Glazner		
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	ITC Transmission	Elizabeth Howell	Affirmative	
1	JEA	Ted E. Hobson	Abstain	
1	Kansas City Power & Light Co.	Michael Gammon		
1	Kissimmee Utility Authority	Joe B Watson	Affirmative	
1	Lakeland Electric	Larry E Watt	Abstain	
1	Lincoln Electric System	Doug Bantam		
1	MEAG Power	Danny Dees	Affirmative	
1	National Grid	Manuel Couto		
1	Nebraska Public Power District	Richard L. Koch	Abstain	
1	New York Power Authority	Ralph Rufrano	Affirmative	
1	New York State Electric & Gas Corp.	Henry G. Masti	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Abstain	
1	Oncor Electric Delivery	Charles W. Jenkins		
1	Pacific Gas and Electric Company	Chifong L. Thomas	Affirmative	
1	PacifiCorp	Mark Sampson		
1	Potomac Electric Power Co.	Richard J. Kafka	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Negative	
1	PP&L, Inc.	Ray Mammarella	Affirmative	
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	SaskPower	Wayne Guttormson	Abstain	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Affirmative	
1	Tri-State G & T Association Inc.	Keith V. Carman	Abstain	
1	Westar Energy	Allen Klassen	Affirmative	
1	Xcel Energy, Inc.	Gregory L. Pieper	Affirmative	
2	Alberta Electric System Operator	Anita Lee		
2	BC Transmission Corporation	Faramarz Amjadi	Abstain	
2	California ISO	Greg Tillitson	Abstain	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Affirmative	
2	Midwest ISO, Inc.	Terry Bilke	Affirmative	
2	New Brunswick System Operator	Alden Briggs		
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Affirmative	
3	Alabama Power Company	Bobby Kerley	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana	Affirmative	
3	Arizona Public Service Co.	Thomas R. Glock	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	City Public Service of San Antonio	Edwin Les Barrow	Abstain	
3	Commonwealth Edison Co.	Stephen Lesniak	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	David A. Lapinski	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Jalal (John) Babik	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy Services, Inc.	Matt Wolf	Affirmative	View
3	FirstEnergy Solutions	Joanne Kathleen Borrell	Affirmative	

3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Leslie Sibert	Affirmative	
3	Georgia System Operations Corporation	Edward W Pourciau	Abstain	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Sam Kokkinen		
3	Gulf Power Company	Gwen S Frazier	Affirmative	
3	Hydro One Networks, Inc.	Michael D. Penstone	Affirmative	
3	JEA	Garry Baker	Abstain	
3	Kansas City Power & Light Co.	Charles Locke		
3	Lincoln Electric System	Bruce Merrill	Abstain	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Abstain	
3	Mississippi Power	Don Horsley	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Abstain	
3	New York Power Authority	Michael Lupo	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters	Abstain	
3	PacifiCorp	John Apperson	Abstain	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	View
3	Public Utility District No. 2 of Grant County	Greg Lange	Negative	
3	Sacramento Municipal Utility District	Mark Alberter	Abstain	
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson		
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin L Holt		
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Northern California Power Agency	Fred E. Young	Abstain	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R. Wallace	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Abstain	
5	AEP Service Corp.	Brock Ondayko		
5	Amerenue	Sam Dwyer	Affirmative	
5	Avista Corp.	Edward F. Groce	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Colmac Clarion/Piney Creek LP	Harvie D. Beavers	Affirmative	
5	Constellation Power Source Generation, Inc.	Scott A Etnoyer	Abstain	
5	Consumers Energy	James B Lewis	Affirmative	
5	Detroit Edison Company	Ronald W. Bauer	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	View
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	FPL Energy	Benjamin Church	Negative	
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	JEA	Donald Gilbert	Abstain	
5	Kansas City Power & Light Co.	Scott Heidtbrink		
5	Lincoln Electric System	Dennis Florom		
5	Louisville Gas and Electric Co.	Charlie Martin	Abstain	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Abstain	
5	Northern States Power Co.	Liam Noailles	Affirmative	
5	Orlando Utilities Commission	Richard Kinas	Abstain	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp Energy	David Godfrey	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Abstain	
5	PPL Generation LLC	Mark A. Heimbach	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	

5	PSEG Power LLC	Thomas Piascik	Affirmative	View
5	Salt River Project	Glen Reeves	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	South Carolina Electric & Gas Co.	Richard Jones	Affirmative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	View
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Negative	View
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Thomas Saitta		
6	Lincoln Electric System	Eric Ruskamp	Abstain	
6	Louisville Gas and Electric Co.	Daryn Barker	Abstain	
6	Luminant Energy	Thomas Burke		
6	New York Power Authority	Thomas Papadopoulos	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Abstain	
6	PacifiCorp	Gregory D Maxfield	Affirmative	
6	PP&L, Inc.	Thomas Hyzinski	Affirmative	
6	Progress Energy	James Eckelkamp	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Southern California Edison Co.	Marcus V Lotto	Affirmative	
6	Tampa Electric Co.	Joann Wehle		
6	Western Area Power Administration - UGP Marketing	John Stonebarger		
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8	Edward C Stein	Edward C Stein	Affirmative	
8	James A Maenner	James A Maenner	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Roger C Zaklukiewicz	Roger C Zaklukiewicz	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
8	Wally Magda	Wally Magda	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	Maine Public Utilities Commission	Jacob A McDermott	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G Dvorsky		
9	Public Utilities Commission of Ohio	Klaus Lambeck		
10	Electric Reliability Council of Texas, Inc.	Kent Saathoff	Affirmative	
10	Midwest Reliability Organization	Dan R Schoenecker	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Jacquie Smith	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	

Account Log-In/Register

Exhibit C

Standard Drafting Team Roster

Order 706B Nuclear Implementation Plan Standard Drafting Team

David R. Ambrose SCADA System Manager	Western Area Power Administration - Rocky Mountain Region 5555 E. Crossroads Blvd. Loveland, Colorado 80538	(970) 461-7354 (970) 461-7213 Fx ambrose@wapa.gov
Jay Amin Cyber Security Program Manager	Luminant Power P.O. Box 1002 Glen Rose, Texas 76043-1002	(254) 897-6469 (254) 897-6777 Fx jamin1@luminant.com
Chuck L. Behrend Director of Corporate Design Engineering	Exelon Nuclear 200 Exelon Way Kennett Square, Pennsylvania 19348	(610) 765-5910 (610) 765-5651 Fx chuck.behrend@exeloncorp.com
Sandra Bittner		sandra.bittner@aps.com
Larry Bugh Chief Security Officer	ReliabilityFirst Corporation 320 Springside Drive — Suite 300 Akron, Ohio 44333	(330) 247-3046 (330) 456-3648 Fx larry.bugh@rfirst.org
David Burford Manager, Nuclear Fleet Security and Emergence Preparedness	Southern Company 40 Iverness Center Parkway Birmingham, Alabama 35242	(205) 992-7315 dpburfor@southernco.com
James Busbin Supervisor - Bulk Power Operations (System Dispatcher)	Southern Company Services, Inc. 600 N. 18th Street Birmingham, Alabama 35291-2625	(205) 257-6357 (205) 257-6663 Fx jybusbin@southernco.com
Marc Marion Butts	Southern Company Services, Inc. 600 North 18th Street — P.O. Box 2641 Birmingham, Alabama 35291-2625	(205) 257-4839 (205) 257-6663 Fx mmbutts@southernco.com
Keith Cooke CIO	Entergy Northwest MD 1480 — P.O. Box 968 Richland, Washington 99352	(509) 377-8334 kscooke@entergy-northwest.com
David M. Czufin		david.czufin@exeloncorp.com
Jeff Drowley		jeff.drowley@exeloncorp.com
Thomas R. Flowers President	Flowers Control Center Solutions 9338 Clark Road Todd Mission, Texas 77363	(936) 894-3649 flowersccs@att.net
David Gambrell Chief Engineer	Southern Company 40 Iverness Center Parkway — Bin B030 Birmingham, Alabama 35242	(205) 992-6480 (205) 992-5465 Fx dlgambre@southernco.com
William R Gross Manager, Web Services	Nuclear Energy Institute	202 739 8123 wrg@nei.org
R. Scott Henry Vice President, Electric Systems Operations	Duke Energy 526 S. Church Street — P.O. Box 1006 Charlotte, North Carolina 28201-1006	(704) 382-6182 (980) 373-5393 Fx scott.henry2@duke-energy.com
Mark J Kuras Senior Engineer	PJM Interconnection, L.L.C. 955 Jefferson Ave Valley Forge Corporate Center Norristown, Pennsylvania 19403	610-666-8924 610-666-4779 Fx kuras@pjm.com

Eric J. Lee Security Specialist 1	U.S. Nuclear Regulatory Commission TWFN 11545 Rockville Pike Rockville, Maryland 20852	(301) 415-8099 (301) 415-5440 Fx exl@nrc.gov
John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place — Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
Alison MacKellar NERC Compliance Contact	Exelon Nuclear — Licensing — 4th Floor 4300 Winfield Road Warrenville, Illinois 60555	(630) 657-2817 (630) 657-4327 Fx alison.mackellar@exeloncorp.com
David McPhail Attorney	Balch & Bingham 1710 Sixth Avenue N. P.O. Box 306 Birmingham, Alabama 35203	(205) 226-8778 (205) 488-5875 Fx dmcphail@balch.com
Michael Mertz Technology and Risk Management	Southern California Edison Co.	(626) 543-6104 Michael.Mertz@sce.com
Margaret M. Miller Director, IT Security and Compliance	Exelon Corporation 10 S. Dearborn — 45th Floor Chicago, Illinois 60603	(312) 394-3743 (312) 394-8888 Fx margaret.miller@exeloncorp.com
George T. Miserendino President	Triton Security Solutions, Inc. 4959 138th Circle W. Apple Valley, Minnesota 55124-9229	(952) 210-5563 (952) 322-2505 Fx george@tritonsecsol.com
Scott Morris Deputy Director for Reactor Security	U.S. Nuclear Regulatory Commission 11555 Rockville Pike — Mail Stop T4-F25M Rockville, Maryland 20852	(301) 415-7083 (301) 415-5440 Fx scott.morris@nrc.gov
Steven T. Naumann Vice President, Wholesale Market Development	Exelon Corporation — Chase Tower 10 S. Dearborn Street - 53rd Floor Chicago, Illinois 60603	(312) 394-2807 (312) 394-2101 Fx steven.naumann@exeloncorp.com
Andrew Neal Senior Engineer	Southern Nuclear Company 42 Iverness Center — P.O. Box 1295 Birmingham, Alabama 35201	(205) 992-7662 aaneal@southernco.com
David L. Norton Policy Consultant - CIP	Entergy Corporation 639 Loyola Avenue — MS: L-MOB-17A New Orleans, Louisiana 70113	(504) 576-5123 (504) 576-5123 Fx dnorto1@entergy.com
Howard Lee Owrutsky IT Manager - Nuclear Site Support	Exelon Corporation TMI Training Center Building 2 Route 441 South Middletown, Pennsylvania 17057	(717) 948-2020 howard.owrutsky@exeloncorp.com
Bonnie R. Parker It Manager	Southern Company Services, Inc. 600 North 18th Street — Bin 5N-8424 Birmingham, Alabama 36203	(205) 257-1624 (205) 257-3689 Fx
Phil Prugnarola Director, IM Business Solutions - Nuclear	NextEra Energy Resources, LLC	(603) 773-7240 phil.prugnarola@nexteraenergy.com
Jack W. Roe Director, Security	Nuclear Energy Institute 1776 I Street N.W. — Suite 400 Washington, D.C. 20006	(202) 739-8138 jwr@nei.org
John C. Rommel		john.rommel@exeloncorp.com

Neil Saia		504-576-4792 nsaia@entergy.com
James W. Sample Director of Cyber Security	Tennessee Valley Authority 1101 Market Street — Mailstop: SP 5A-C Chattanooga, Tennessee 37402-2801	(423) 751-4794 (423) 751-6858 Fx jwsample@tva.gov
Steve Swanson		scswanso@southernco.com
Robert Sypult President	RLS Security Advisors 2815 Sierra Canyon Way Hacienda Heights, California 91745	(626) 333-6765 (626) 333-6765 Fx rlsypult@aol.com
Howard Tarler Consultant	Electric Power Engineering 35 Fairway Court Albany, New York 12208	(518) 489-9134 (518) 489-9136 Fx htarler1@nycap.rr.com
Thomas Turke Director of Corporate Compliance	Seminole Electric Cooperative, Inc. 16313 N. Dale Mabry Hwy. Tampa, Florida 33688	(813) 739-1244
Chris Wilson Engineer	Southern Company 600 18th Street North Birmingham, Alabama 35291	(205) 257-4241 cmwilson@southernco.com
Bradley Yeates IT Security Analyst, Principal	Southern Company 241 Ralph McGill Boulevard — Bin 10030 Atlanta, Georgia 30308	(404) 506-3886 (404) 505-6277 Fx blyeates@southernco.com
Julia York Transmission Policy Analyst	Southern Company Services, Inc. 600 N. 18th Street — Bin 13N-8812 P.O. Box 2641 Birmingham, Alabama 35291	(205) 257-5196 (205) 257-6654 Fx jlyour@southernco.com
Jason Zorn		jason.zorn@nrc.gov
Gerard Adamski — NERC Vice President and Director of Standards	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx gerry.adamski@nerc.net
Roger Lampila — NERC Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx roger.lampila@nerc.net
Scott R Mix — NERC Manager Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(6090 452-8060 (609) 452-9550 Fx Scott.Mix@nerc.net
Tim E. Roxey — NERC Manager of Critical Infrastructure Protection	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx tim.roxey@nerc.net