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.			