Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

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

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–002–2 — Cyber Security — Critical Cyber Asset Identification and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-2

3. Purpose: NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

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

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

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-2:

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

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

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

B. Requirements

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

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

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

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

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

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

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

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

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

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

R2. 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.

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-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

1.5.1 None.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

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

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–003–2 — Cyber Security – Security Management Controls and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-2

3. Purpose: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-003-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-2:

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

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

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

B. Requirements

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

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

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

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

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.

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

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

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

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

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

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

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

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

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

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

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

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

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

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

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

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

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

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

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

C. Measures

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

1.5.1 None

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Changed compliance monitor to Compliance Enforcement Authority.	
	04 Feb 2009	Modifications to clarify the requirements and to incorporate industry comments. Section 1.5: Additional Compliance Information, added “None” Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing	

		access (removed the business phone information).	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

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

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–002–4 — Cyber Security — Personnel and Training and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-2

3. **Purpose:** Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. **Applicability:**

   4.1. Within the text of Standard CIP-004-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-004-2:

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

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

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

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

- Management support and reinforcement (e.g., presentations, meetings, etc.).

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

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

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

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

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

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

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

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

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

The personnel risk assessment program shall at a minimum include:

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

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

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-2.

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

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

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

C. Measures

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Removal of 90 day window to complete training and personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
	4 Feb 2009	Modifications to clarify the requirements and to incorporate industry comments. Modification to R1 for the awareness and training program to establish, document, implement, and maintain**.** Modification to R2 stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

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

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–005–2 — Cyber Security — Electronic Security Perimeter(s) and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

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

2. Number: CIP-005-2

3. Purpose: Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-2:

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

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

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

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

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

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

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-2.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.

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

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

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

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

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

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

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

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

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.

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

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

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

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

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

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

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

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

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

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

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

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.

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

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

C. Measures

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-2, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-2 from the previous full calendar year.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity.	

		Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Deleted the word "dated" from the Measures.	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

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

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–006–2 — Cyber Security — Physical Security and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

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

2. **Number:** CIP-006-2

3. **Purpose:** Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. **Applicability:**

   4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-006-2:

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

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

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

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

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

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

R1.4. Appropriate use of physical access controls as described in Requirement ~~R3~~ R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

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

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

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

R2.1. Be protected from unauthorized physical access.

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

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

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

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

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:

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

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

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

R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

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

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

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

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

C. Measures

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

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

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

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

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

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

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

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

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

1.5. Additional Compliance Information

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

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-2 for that single access point at the dial-up device.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Modify Physical Security Plan to document, implement, and maintain. Correct Requirement reference in R1.4 to R4	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

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

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–007–2 — Cyber Security — Systems Security Management and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-2

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-2:

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

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. 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-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

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

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

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

1.5. Additional Compliance Information.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Replaced the RRO with the RE as a responsible	

		entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Revise the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter.	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

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

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–008–2 — Cyber Security — Incident Reporting and Response Planning and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-2

3. Purpose: Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-008-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-2:

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

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

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its ~~dated~~ Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entity.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-2 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Removed “dated” from Measure M1.	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

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

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for Critical Cyber Assets

2. **Number:** CIP-009-2

3. **Purpose:** Standard CIP-009-2 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. **Applicability:**

   4.1. Within the text of Standard CIP-009-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator

   4.1.2 Balancing Authority

   4.1.3 Interchange Authority

   4.1.4 Transmission Service Provider

   4.1.5 Transmission Owner

   4.1.6 Transmission Operator

   4.1.7 Generator Owner

   4.1.8 Generator Operator

   4.1.9 Load Serving Entity

   4.1.10 NERC

   4.1.11 Regional Entity

   4.2. The following are exempt from Standard CIP-009-2:

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

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

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

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

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:~~

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its ~~dated~~ recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its ~~dated~~ records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its ~~dated~~ documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its ~~dated~~ documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its ~~dated~~ documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.1.2 ERO for Regional Entities.

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

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.5. Additional Compliance Information

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

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Revised the wording in Section B, Requirements, to be consistent with the other standards. Remove “dated” from the measures.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments on 1st Draft of CIP-002-2 through CIP-009-2 — Project 2008-06 — Cyber Security Order 706

The Cyber Security for Order 706 Standard Drafting Team thanks all commenters who submitted comments on the first draft of following CIP standards:

CIP–002–2 — Cyber Security — Critical Cyber Asset Identification
CIP–003–2 — Cyber Security — Security Management Controls
CIP–004–2 — Cyber Security — Personnel and Training
CIP–005–2 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–2 — Cyber Security — Physical Security
CIP–007–2 — Cyber Security — Systems Security Management
CIP–008–2 — Cyber Security — Incident Reporting and Response Planning
CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards were posted for a 45-day public comment period from November 21, 2008 through January 5, 2009. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 52 sets of comments, including comments from more than 100 different people from over 55 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

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

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

Index to Questions, Comments, and Responses

The Industry Segments are:

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

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Individual	Kent Kujala	Detroit Edison Company			✓		✓					
2.	Individual	Paul Golden	PacifiCorp	✓		✓		✓					
3.	Group	Doug Hohlbaugh	FirstEnergy Corp	✓		✓	✓	✓	✓				
4.	Individual	Ray Andrews	MidAmerican Energy Company	✓		✓		✓					
5.	Group	Guy Zito	Northeast Power Coordinating Council										✓

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	1, 3, 4, 5, 6
2.	Terry Malone	FE	RFC	1, 3, 4, 5, 6
3.	Karen Yoder	FE	RFC	1, 3, 4, 5, 6
4.	Dave Folk	FE	RFC	1, 3, 4, 5, 6
5.	Henry Stevens	FE	RFC	1, 3, 4, 5, 6

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Edward Dahill	National Grid	NPCC	3
2.	Gerald Mannarino	NYPA	NPCC	5
3.	Frederick White	Northeast Utilities	NPCC	1
4.	Michael Garton	Dominion Resources Services, Inc.	NPCC	5
5.	Kathleen Goodman	ISO - New England	NPCC	2
6.	Michael Gildea	Constellation Energy	NPCC	6
7.	Donald Nelson	Massachusetts Dept. of Public Utilities	NPCC	9
8.	Roger Champagne	Hydro-Quebec TransEnergie	NPCC	1
9.	David Kiguel	Hydro One Networks Inc.	NPCC	1
10.	Brian Hogue	NPCC	NPCC	10
11.	Gerry Dunbar	NPCC	NPCC	10
12.	Lee Pedowicz	NPCC	NPCC	10
13.	Brian Evans-Mongeon	Utility Services	NPCC	6

6.	Individual	Linda Perez	WECC Reliability Coordination										✓
7.	Group	Marc M. Butts	Southern Company	✓		✓		✓	✓				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rodney O'Bryant	Southern Company Services	SERC	1
2.	Larry Spoonemore	Southern Company Services	SERC	5
3.	Jim Busbin	Southern Company Services	SERC	1
4.	Bonnie Parker	Southern Company Services	SERC	5
5.	Boyd Nation	Southern Company Services	SERC	1
6.	Wes Stewart	Southern Company Services	SERC	1
7.	Bob Canada	Southern Company Services	SERC	1
8.	Wade Mundy	Southern Company Services	SERC	1
9.	John Greaves	Georgia Power Company	SERC	1, 3

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10
	10. Jay Cribb	Southern Company Services	SERC	1								
	11. Chris Wilson	Southern Company Services	SERC	1								
	12. Terry Coggins	Southern Company Services	SERC	1								
	13. Russ Ward	Southern Company Services	SERC	1								
	14. Steve Bennett	Georgia Power Company	SERC	1, 3								
	15. Larry Smith	Alabama Power Company	SERC	1, 3								
8.	Individual	Rick Terrill	Luminant Power					✓					
9.	Group	Matthew E. Luallen	Encari								✓		
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
	1. Steve Hamburg	Encari	NA - Not Applicable	8									
	2. Mark Simon	Encari	NA - Not Applicable	8									
	3. Lenny Mansell	Encari	NA - Not Applicable	8									
	4. Peter Brown	Encari	NA - Not Applicable	8									
10.	Individual	Mark Phillips	TransAlta Centralia Generation, LLC					✓					
11.	Group	Denise Koehn	Bonneville Power Administration	✓		✓		✓	✓				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
	1. Curt Wilkins	Transmission System Operations	WECC	1									
	2. Bradley Folden	Transmission Technical Training	WECC	1									
	3. Kelly Hazelton	Transmission Control Cntr HW Design & Maint	WECC	1									
12.	Individual	John Lim	Consolidated Edison Company of New York, Inc.	✓		✓		✓	✓				
13.	Individual	Rebecca Furman	Southern California Edison Company	✓		✓		✓	✓				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
14.	Individual	T.J. Szelistowski	Tampa Electric Company	✓		✓		✓					
15.	Group	Jalal Babik	Electric Market Policy	✓		✓		✓	✓				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Louis Slade	Electric Market Policy	RFC	6
2.	Mike Garton	Electric Market Policy	NPCC	5
3.	Mark Engels	IT Risk Management	SERC	
4.	Ruth Blevins	IT Risk Management	SERC	
5.	Dennis Sollars	IT Risk Management	SERC	
6.	John Albert	Security Compliance	SERC	

16.	Group	Annette M. Bannon	PPL Corporation	✓				✓	✓				

Please complete the following information.

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Heimbach	PPL EnergyPlus	MRO	6
2.			NPCC	6
3.			RFC	6
4.			SERC	6
5.			SPP	6
6.	Jim Batug	PPL Generation	NPCC	5
7.			RFC	5
8.			WECC	5
9.	Barry Skoras	PPL Electric Utilities	RFC	1

17.	Group	Michael Brytowski	MRO NERC Standards Review Subcommittee										✓

	Additional Member	Additional Organization	Region	Segment Selection
1.	Neal Balu	WPS	MRO	3, 4, 5, 6

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10
	2. Terry Bilke	MISO	MRO	2								
	3. Carol Gerou	MP	MRO	1, 3, 5, 6								
	4. Jim Haigh	WAPA	MRO	1, 6								
	5. Charles Lawrence	ATC	MRO	1								
	6. Ken Goldsmith	ALTW	MRO	4								
	7. Terry Harbour	MEC	MRO	1, 3, 5, 6								
	8. Pam Sordet	XCEL	MRO	1, 3, 5, 6								
	9. Dave Rudolph	BEPC	MRO	1, 3, 5, 6								
	10. Eric Ruskamp	LES	MRO	1, 3, 5, 6								
	11. Joseph Knight	GRE	MRO	1, 3, 5, 6								
	12. Larry Brusseau	MRO	MRO	10								
	13. Scott Nickels	RPU	MRO	3, 4, 5, 6								
18.	Group	Richard Kafka	Pepco Holdings, Inc - Affiliates		✓		✓		✓	✓				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**								
	1. Mark Godfrey	Pepco Holdings, Inc.	RFC	1								
19.	Individual	Michael Puscas	United Illuminating Company		✓		✓							
20.	Individual	Steven Dougherty	Deloitte& Touché, LLP											
21.	Individual	Chris Scanlon	Exelon		✓		✓		✓	✓				
22.	Individual	Mark Ringhausen	Old Dominion Electric Cooperative					✓						
23.	Individual	Alan Gale	City of Tallahassee (TAL)		✓		✓		✓					
24.	Individual	Brian Martin	BC Transmission Corporation		✓	✓								
25.	Individual	Joe Weiss	Applied Control Solutions, LLC											

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
26.	Individual	Martin Bauer	US Bureau of Reclamation	✓				✓					
27.	Individual	Edward Bedder	Orange and Rockland Utilities Inc.	✓									
28.	Individual	Martin Narendorf	CenterPoint Energy	✓									
29.	Individual	Kris Manchur	Manitoba Hydro	✓	✓		✓	✓					
30.	Individual	Anita Lee	Alberta Electric System Operator		✓								
31.	Individual	Greg Mason	Dynegy					✓					
32.	Individual	Tim Conway	Northern Indiana Public Service Company	✓		✓		✓					
33.	Individual	Robert Huffman	CoreTrace								✓		
34.	Individual	Darryl Curtis / Greg Ward	Oncor Electric Delivery LLC	✓									
35.	Individual	Bob Thomas	Illinois Municipal Electric Agency				✓						
36.	Individual	Cathie Mellerup	Ontario Power Generation					✓					
37.	Individual	Jim Sorrels	American Electric Power	✓		✓		✓	✓				
38.	Individual	Dan Rochester	Ontario IESO		✓								
39.	Individual	Kirit Shah	Ameren	✓		✓		✓	✓				
40.	Individual	Jianmei Chai	Consumers Energy Company			✓	✓	✓					
41.	Individual	Alice Druffel	Xcel Energy	✓		✓		✓	✓				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
42.	Individual	Kathleen Goodman	ISO New England Inc		✓								
43.	Individual	Jason Shaver	American Transmission Company	✓									
44.	Individual	James W. Sample	TVA	✓		✓		✓	✓				
45.	Individual	Greg Rowland	Duke Energy	✓		✓		✓	✓				
46.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	✓									
47.	Group	Ed Goff	Progress Energy	✓		✓		✓	✓				
48.	Group	Ben Li	Standards Review Committee of ISO/RTO Council										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Patrick Brown	PJM	NPCC	2
2.	Jim Castle	NYISO	NPCC	2
3.	Matt Goldberg	ISONE	NPCC	2
4.	Lourdes Estrada-Salinero	CAISO	WECC	2
5.	Anita Lee	AESO	WECC	2
6.	Steve Myers	ERCOT	ERCOT	2
7.	Bill Phillips	MISO	RFC	2
8.	Charles Yeung	SPP	SPP	2

49.	Individual	Aldo Nevarez	KEMA										
50.	Individual	Dave DeGroot	Austin Energy	✓				✓					

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
51.	Individual	Glen Hattrup	Kansas City Power & Light	✓		✓		✓					
52.	Individual	Randy Schimka	San Diego Gas and Electric Co.	✓		✓	✓	✓					

1. The CSO706 SDT added management approval of the risk-based assessment methodology (per FERC Order 706, paragraph 236) to **CIP-002-1 Requirement R4**. Do you agree with the proposed modification? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 1 Comment
Detroit Edison Company	Yes	
PacifiCorp	Yes	
FirstEnergy Corp	Yes	
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	No	We recommend that CIP-002 be updated by moving CIP-003 R2 into CIP-002. By moving CIP-003 R2 into CIP-002 all the Requirements that all Entities must complete are in one Standard. The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into the CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
WECC Relibaility Coordination	Yes	
Southern Company	Yes	CIP-002 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority.

Organization	Yes or No	Question 1 Comment
		CIP-002 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-002 Section D - Compliance: 1.4.2- Should have a time limit to reduce the overall liability of confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.2 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. R4 should also include a direct reference to CIP-003-2 R2 to ensure that the Responsible Entities are aware are all applicable requirements. A Responsible Entity that identifies a null CA list must still perform CIP-003-1 R2. This would allow the exemption in CIP-003-2 (4.2.3) to be removed. General Comment Provided in All Submissions--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Organization	Yes or No	Question 1 Comment
Response: **1. The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2. The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **3. The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.** **The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	We agree with the proposed modification, but have suggestions which affect CIP-002 in one area of the Leadership requirement which would be more logical.CIP-002 requires the approval of the Senior Manager for many requirements, and is the standard that determines whether other CIP standards are applicable to the Entity. In order to streamline compliance filing in these cases, and also as a more logical place for the identification of a Senior Manager, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard.1 - The senior manager has not been identified in CIP-002. Many requirements make

Organization	Yes or No	Question 1 Comment
		reference to the Senior Manager or delegate. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone. This is the preferred option.Or2 - The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements shall?
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Southern California Edison Company	Yes	
Tampa Electric Company	Yes	
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Propose that section 4.2 for each standard (CIP-002-2 through CIP-009-2) be updated to state that law enforcement agencies and emergency services in the performance of their duties are exempt from the standards.
Response: **1) NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **2) Law enforcement agencies and emergency services are not users, owners, or operators of the Bulk Power System; therefore, it is not necessary to exempt them. Their access should be included in the emergency provisions of the cyber security policy as required by the Emergency Situations Provision in CIP-003-R1.1.**		
PPL Corporation	Yes	
MRO NERC Standards	No	The MRO NSRS believes that R4 is prescriptive in nature. The requirement tells how to accomplish, not

Organization	Yes or No	Question 1 Comment
Review Subcommittee		what to accomplish.
Response: **The SDT respectfully disagrees with the comment. CIP-002-2 R4 is a requirement for governance over the critical cyber asset identification standard. The SDT's intent was to define annual approval by the senior manager.**		
Pepco Holdings, Inc - Affiliates	No	We appreciate and support the CSO706 SDT efforts. We agree and support the following proposed changes in CIP-002-2 through CIP-009-2: 1. Nomenclature and clarification changes (e.g. changing RRO to Regional Entity, version references) 2. Clearly state that requirements not only need a program but need to be implemented (e.g. electronic access controls, awareness program, Security Patch Management program) 3. Removed the term "reasonable business judgment" 4. Where applicable, removed the phrase "acceptance of risk" 5. Added annual review and approval of risk-based assessment methodology 6. Background checks and training would be required prior to allowing unescorted physical access or cyber access to critical cyber assets (i.e. eliminates 90 days or 30 days after the fact but allows for emergencies) 7. Added protection of physical access control systems However we have the following questions about changes in CIP-002-2. (These questions also apply to CIP-003-2 through CIP-009-2 but will not be repeated below.): 1). The proposed change for D. Compliance, Section 1.1 appears to add a new term, "Compliance Enforcement Authority", (which we do not believe is in the Glossary of Terms or in any other standards as of 12/1/08). Does the CSO706 SDT plan to define this new term? If yes, how will it be different from the term "Compliance Monitor" (defined in the Glossary of Terms)? 2). In D. Compliance, Section 1.1.2 The proposed change is to replace NERC with ERO. We believe that this should be left as NERC as we do not believe ERO appears in the Glossary of Terms or in any other standards. If ERO remains, does ERO need to be added to the applicability list in A. Introduction, Section 4.1 and the Glossary of Terms?
Response: **1) The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term,**		

Organization	Yes or No	Question 1 Comment
"Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures. **2) Under the ERO Rules of Procedure, the ERO can be penalized but not NERC – therefore the use of the term, "Electric Reliability Organization" or "ERO" is technically correct. As a guideline, drafting teams are asked not to add terms to the glossary unless there is a chance that the term will be misunderstood. In this case, the entities who follow these standards should know what is meant by these terms, and we don't believe the terms need to be added to the glossary.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	While I agree with the R4 revision, I disagree with the removal of the "reasonable business judgement" in all the standards. While this was in response to FERC directive, it creates a one-size-fits-all approach. Every system is different, as is their Risk Assessment Procedure. This will be one of the more contentious issues. While it may be outside the perview of the SDT, the industry has not been given the information that is needed to specifically address the Auroura fiasco. All we know is someone set up a generator and "hacked" in to change the set frequency and damage ensued. We are not aware of what software was in place to protect this "asset" or what controlling software was. Can the specifics of who set up the test and the hardware/software/control systems being utilized be shared with the industry through a NERC Alert Industry Advisory? While I do not think I have my head buried in the sand about the potential for Cyber attack, I do have a problem with taking all-encompassing action with so little information on what caused the initial knee-jerk reaction. The cost of safeguarding a system against such unknown attacks, to a level that will be acceptable during an audit (a second unknown) will surely be a significant burden to many utilities. While entities have some latitude in our "methodology" in identifying Critical Assets, the fact will remain that you have to spend money on new tools and hardware to comply with the existing requirements outside of routine budget cycles at a significant impact to operations. According to the letter from Rick

Organization	Yes or No	Question 1 Comment
		Sergel to the BOT of July 7, 2008 even after we spend a ton of money, we are still susceptible to attack. Without the flexibility of determining cost vs. benefit, we will overachieve the goal of ".. .reasonably ensure the reliability of the BPS. . ."
Response: **The comments concerning Aurora are outside of the aegis of the SDT.** **The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	No	Need to include the NIST Framework in addition to senior management approval
Response: **The SDT plans to consider the NIST Framework during future phases of standards review, as directed by FERC Order 706.**		
US Bureau of Reclamation	No	The modification of the standard to require that a specific individual approve the risk-assessment methodology appears to be overstepping the bounds of the authority of the regulatory agencies as it pertains to improved reliability. It is difficult to imagine or prove that having one individual within an agency approve a methodology (as opposed to making the entity responsible for having and using a methodology) improves system reliability. Such a requirement is also not consistent with most of the other BES reliability standards. For consistency, the standard should refer to "Responsible Entity" rather than specific individuals within the organization. That determination is the sole discretion of the Responsible Entity and was not required by FERC. FERC required, in paragraph 236, that "internal, management, approval of the riskbased assessment" is required. FERC further clarified: "A responsible entity, however, remains responsible to identify the critical assets on its system". To that end the standard should require that the 'Responsible Entity" ensure that management has approved the risk based assessment. The "Responsible Entity" is then responsible to demonstrate that the requirement has been met and who approved it.

Organization	Yes or No	Question 1 Comment
Response: **The intent of the standard is not to define an entity's organizational structure. The intent is to ensure that the appropriate governance structure is taken into consideration and that, as directed by FERC, there exists a single individual with overarching authority.**		
Orange and Rockland Utilities Inc.	No	We recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard.1 – The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone.2 - The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements shall?
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator	No	The functional entity (e.g. the Balancing Authority, etc) should be designated as the responsible entity for this requirement, not an individual. This would be consistent with other ERO standards. Also, R1 implies that the purpose of this standard is not only to identify the "Critical Cyber Assets" but also the "Critical Assets" (which must be done before you can identify the Critical Cyber Assets), and hence we suggest that either the identification of "critical Assets" be specified in its own and separate standard or the Title and Purpose of CIP-002 be clarified to state that there are 2 purposes to this standard. We suggest that R1 should be re-written to improve clarity. R1, as currently written, contains not only a single requirement, but with at least two, and possibly three or more requirements embedded in it. The accountabilities for these different requirements could be different within an organization, so assigning them to one person would be inappropriate.

Organization	Yes or No	Question 1 Comment
Response: **The change made in CIP-002 includes adding the management approval of the risk-based assessment methodology per directives in FERC Order 706. Given the limited scope and timeline for Phase 1, please readdress the additional concerns during the Phase 2 comment period.**		
Dynegy	No	Agree with requiring management approval of the risk-based assessment methodology. Also, suggest moving CIP-003, R2 into CIP-002 so that all the Requirements that all Entities must comply with are in one Standard.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Northern Indiana Public Service Company	No	I do support the recommended change to require management approval of the risk-based assessment methodology per FERC Order 706, paragraph 236. I would like to recommend the addition of some language to CIP-002-2 Req 4. Currently the language in R4 directs the responsible entity to comply with CIP-002-2 R1-R3 and retain a record of the resulting CA and CCA asset list (even if that list is null). My concern is that if the list is null the entity may feel they have completed all necessary actions for compliance. There is however compliance actions for an entity with a null list contained within CIP-003-2. As it stands there is an oddly placed exemption in the applicability section of CIP-003 4.2.3. I would recommend the inclusion of language in CIP-002-2 Req. 4 to identify the need for compliance with CIP-003-2 R2 as well as the currently referenced CIP-002-2 R1-3; in order to contain all applicability for CIP-002-2 R4 in one location and in turn removing the exemption in CIP-003-2. As there is no other means through the use of this comment form I would also like to comment on changes made in CIP-002-2 that repeat throughout CIP-002-2 - CIP-009-2 In the purpose section of CIP-002-2, I would like to see as a component of this draft, an attempt to develop alternative language to replace reasonable business judgment as mentioned in Order 706 in paragraph 135. In the Data Retention section of CIP-002-2, I would like to request clarification on the language added to 1.4.2. As the language was there was a limit on data retention that matched the audit enforcement

Organization	Yes or No	Question 1 Comment
		period of three years. The language provided currently removes this limit and extends the retention into perpetuity as well as leaving it unclear which entity is responsible for retaining the data into perpetuity.

Response:

The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.

The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.

The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.

CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency	Yes	
Ontario Power Generation	No	Measures M2 and M3 add a requirement by specifying the lists of Critical Assets and Critical Cyber Assets must be dated. M2 references Requirement R2 and M3 references Requirement R3. Neither R2 or R3 require a list to be dated.

Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
American Electric Power	Yes	Section R4 of the Requirements category does not clearly define what type of unit the senior manager represents. We would suggest a clarifying comment like "for each responsible entity" be added following the word "delegate(s)." This does not appear again in any of the following standards. However, throughout all of these standards, the drafting team has introduced a new term in its use of "Responsible Entity." If this term is to be used, it should probably be considered by the NERC organization with corresponding updates to lists of compliance term glossaries and/or definitions.
Response: **The SDT believes that this change could be too prescriptive and limits the flexibility allowed in delegation.** **"Responsible Entity" is defined within the Applicability section of each CIP standard.**		
Ontario IESO	No	Standards should hold a functional entity(ies) responsible for meeting the requirements, not a person or a position. Furthermore, delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard. We propose R4 be revised to: "Annual Approval? The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) "If appointing a senior manager is required to ensure standards are complied with and implemented, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard.

Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The senior manager is held responsible to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation needs to be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity.**		
Ameren	Yes	None.
Response: **Thank you for your comment.**		
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1) - We recommend that CIP-002 be updated by: moving CIP-003 R2 into CIP-002 or CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. Rational: 2) - The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone. Allows for, "The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements" shall" 3. In this Standard and throughout several other CIP Standards, "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate and cannot be applied.
Response: **1) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in**		

the later phases of the project and resubmit your comments as appropriate if they have not been addressed. **2) The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation should be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity.** **3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
American Transmission Company	Yes	
TVA	No	There are three areas we feel need clarification: 1. Standards should hold a functional entity(ies), not a person or a position, responsible for meeting the requirements; 2. Delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard; and 3. An appointment of a senior manager is a part of CIP-003 and for Responsible Entities without Critical Assets only CIP-002 is applicable. We propose the following: i) R4 be revised to: Annual Approval - The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. ii) The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) iii. Move the senior manager appointment from CIP-003 R2 to CIP-002. Incorporate, by reference to CIP-003, for a senior manager appointment into CIP-002.
Response:		

i) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. (Reference FERC Order 706 Paragraph 381) **ii) The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation should be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity. (reference FERC Order 706, Paragraph 381)** **iii) As stated in CIP-003-2, all Responsible Entities regardless of a null Critical Cyber Asset list are required to perform CIP003-2 R2.**		
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	No	Suggest that the first sentence of R4 be re-written as follows: R4 The Responsible Entity shall assign a single senior manager with overall responsibility and authority for approving annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Progress Energy	Yes	
Standards Review Committee of ISO/RTO Council	No	(1) Standards should hold a functional entity(ies), not a person or a position, responsible for meeting the requirements. Further, delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard. We propose R4 be revised to: "Annual Approval — The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)" If appointing a senior mangager is required to ensure standards are complied with and implemented, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should

		explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. (2) In this Standard and throughout several other CIP Standards, "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate and cannot be applied.
Response: **(1) The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation should be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity.** **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **(2) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

2. The CSO706 SDT is proposing the following modifications to **CIP-003-1**:

   - Revise Applicability 4.2.3 to specify that compliance with Requirement R2 applies to Responsible Entities that have determined they have no Critical Cyber Assets (per FERC Order 706, paragraph 376)
   - Clarify the intent of the Requirement R2 on Leadership that a senior manager be assigned with the overall responsibility and authority for cyber security matters (per FERC Order 706, paragraph 381).
   - Add Requirement R2.3 to address senior manager delegation of authority for specific actions to a named delegate.
   - Renumber the original R2.3 to R2.4.
   - Delete the phrase "or a statement accepting risk" from Requirement R3.2.(per FERC Order 706, paragraph 376)

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 2 Comment
Detroit Edison Company	Yes	
PacifiCorp	No	Suggested modification to R2.3"Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions assigned to the senior manager to a named delegate or delegates."
Response: **The SDT received a number of comments that suggested clarifications to the delegation in CIP-003-2 R2.3. The SDT discussed this specific language and did not agree that it provided clarity over the posted language in the delegation requirement.**		
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	Suggest an addition: The senior may delegate authority for actions assigned to the senior manager in Standards CIP-002-2 through CIP-009-2 to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

Organization	Yes or No	Question 2 Comment
Response: **The SDT believes that the senior manager should annually approve, without delegation, the Cyber Security Policy. As indicated in R2.3, delegation is only allowed where specifically stated in the requirement. Consequently, there is no delegation allowed in the approval of the Cyber Security Policy.**		
Northeast Power Coordinating Council	No	1 - We recommend moving CIP-003 R2 into the CIP-002 Standard. 2 - We request clarification of CIP-003 R2. 3 "the senior manager may delegate authority for specific actions to a named delegate or delegates." Please clarify a) the named delegate(s) and b) the delegation.
Response: **1.-2. The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **3, The SDT believes that the clarifications requested regarding who a delegate is and how a delegation is performed should be determined by the entity, and the SDT does not intend to prescribe a delegation process.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	CIP-003 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-003 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-003 Section D - Compliance: 1.4.2 - Should have a time limit to reduce the overall liability of confidential information.

Organization	Yes or No	Question 2 Comment
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.2 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	Also see comments on Question 1 pertaining to exemption 4.2.3--General Comments Provided in All Submissions--Other modifications were also made to this standard that are not included as part of the question. 1. The wording of 1.1.1 is awkward and should be modified. 2. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. 3. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: **1. The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **2. The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the**		

Organization	Yes or No	Question 2 Comment
Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity. **3. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1) - We recommend moving CIP-003 R2 into the CIP-002 Standard. (See comments to Question 1). 2) - We request clarification of CIP-003 R2. 3) -"the senior manager may delegate authority for specific actions to a named delegate or delegates." 4)- Please clarify a) the named delegate(s) (e.g. does he/she have to be a senior manager?) and b) the requirements for what the delegation must contain (i.e. does it have to explicitly reference the standard and requirement?)
Response: **1)-3) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4) The SDT believes that the clarifications requested regarding who a delegate is and how a delegation is performed should be determined by the entity, and the SDT does not intend to prescribe a delegation process.**		
Southern California Edison Company	No	R1.3 - Add language to indicate whether Senior Manager may or may not delegate annual review and approval of the policy.R3.2 - SCE believes that the removal of "acceptance of risk" limits SCE's ability to analyze risk and determine a proper response. For example, SCE could determine that the residual risk

Organization	Yes or No	Question 2 Comment
		posed by the state of maturity of a technology used to address CIP requirements is both low risk and low probability. Removing the acceptance of risk language would require SCE to continue to allocate time and resources to address the residual risk rather than deeming it acceptable within the CIP Standards. SCE recommends adding language to indicate that where unavoidable residual risk remains after remediation, it must be documented and authorized by the Senior Manager or delegate.
Response: **The SDT believes that the senior manager should annually approve, without delegation, the Cyber Security Policy. As indicated in R2.3, delegation is only allowed where specifically stated in the requirement. Consequently, there is no delegation allowed in the approval of the Cyber Security Policy.** **FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process. [Please refer to FERC 706, Paragraph 151]**		
Tampa Electric Company	No	Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Suggest R3.1 read thirty calendar days.
Response: **1) NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		

Organization	Yes or No	Question 2 Comment
2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	No	The MRO NSRS believes the R2 should be moved to CIP-002. This would package all of the requirements in one standard the apply to every entitiy. The senior may delegate authority for actions assigned to the senior manager in Standards CIP-002-2 through CIP-009-2 to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The SDT believes that the senior manager should annually approve, without delegation, the Cyber Security Policy. As indicated in R2.3, delegation is only allowed where specifically stated in the requirement. Consequently, there is no delegation allowed in the approval of the Cyber Security Policy.** **The SDT received a number of comments that suggested clarifications to the delegation in CIP-003-2 R2.3. The SDT discussed this specific language and did not agree that it provided clarity over the posted language in the delegation requirement.**		
Pepco Holdings, Inc - Affiliates	Yes	We support the proposed modifications including the removal of business phone and business address from B. Requirements, R2.1. Similary, should the business phone requirement be removed from B. Requirements, R5.1.1 - Similar to CIP-002-2, D. Compliance, Section 1.5, should CIP-003-2, D. Compliance, Section 1.5 say "None"?
Response: **Thank you for identifying the inconsistency. Section 1.5 should state, “None”, and “Business phone” in R5.1.1 will be removed.**		
United Illuminating	Yes	

Organization	Yes or No	Question 2 Comment
Company		
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	Although the "acceptance of risk" ties in with the discusson above on business judgement.
Response: **The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	The reference to a senior manager in paragraph 381 was not intended be a requirement. FERC did allow registered entities some flexibility, to wit: "The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve". The modification by the SDT, which specifies delegation by the "senior manager", is intrusive upon the Responsible Entity's organizational structure. It is sufficient to require that the Responsible Entity must be able to produce documentation of who has responsibility for the CIP implementation. For geographically diverse organizations, that responsibility will change depending on the location of the affected systems. Each Responsible Entity generally has identified an individual who is authorized to submit documentation in response to a Regional Entity's requests or through the certification process. The specific requirement

Organization	Yes or No	Question 2 Comment
		that the senior manager have the authority of leading and managing CIP is not the same as requiring certification and may not fit with the organizational lines of the Responsible Entity. Organizational structures must not be legislated in industry standards, especially when the organizations have a vast array of responsibilities and authorities that govern their function. Reclamation has functional responsibilities delegated to Regional Directors in order to manage the vast array of legislated mandates. To require Reclamation to alter its organizational structure in no way improves the reliability of the BES and the requirement appears arbitratry. Each entity certifies that it complies with the integrity of its security through one individual who is authorized to speak for the agency. The requirements should focus on the desired performance outcome which is needed to maintain reliability of the power system, not how the performance is accomplished.
Response: **The SDT believes that R2.3 provides Responsible Entities the flexibility to meet the leadership requirements without prescribing organizational changes.**		
Orange and Rockland Utilities Inc.	No	1) We recommend moving CIP-003 R2 into the CIP-002 Standard. 2) We request clarification of CIP-003 R2. 3) “the senior manager may delegate authority for specific actions to a named delegate or delegates." Please clarify a) the named delegate(s) (e.g. does he/she have to be a senior manager?) and b) the delegation (i.e. does it have to explicitly reference the standard and requirement?)
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The SDT believes that the clarifications requested regarding who a delegate is and how a delegation is performed should be determined by the entity, and the SDT does not intend to prescribe a delegation process.**		
CenterPoint Energy		
Manitoba Hydro	No	In CIP-003 R2.3 the assignment to delegate authority could be done specifically or by assignment through the entitities policies. It should not be necessary to perform specific delegation for all

Organization	Yes or No	Question 2 Comment
		circumstances which necessitates additional overhead for maintaining such documentation of delegation from the senior manager. The webinar on the revisions to the CIP Standards and other recent discussions mentioned the possible creation of a new process for instances when the phrase "where technically feasible" is applied. These instances might also be exceptions to a responsible entity's cyber security policies. Any new process dealing with "where technically feasible" must be supported by additional requirements(s) in the CIP Standards. Responsible Entities should be given direction in the CIPC Standards for identifying, documenting, managing and approving internally these instances. An additional requirement based on CIP-003-1 R3 Exceptions would provide the required direction for industry. Additional requirement(s) must included prior to further industry commenting or balloting on revised CIP Standards or before any new industry process is implemented for "where technically feasible".
Response: **The SDT believes that the clarifications requested regarding how a delegation is performed should be determined by the entity and does not intend to prescribe a delegation process. There is no requirement to delegate.** **The Technical Feasibility Exception process is under development by NERC staff. Please readdress this issue during the Phase 2 comment period.**		
Alberta Electric System Operator	Yes	However, we would like to comment that the responsibility for meeting requirements in standards must lie with the functional entity, not an individual within the entity. Also, we don't believe details on how delegation is done within an entity should be included in a standard. We propose R4 be revised to: "Annual Approval". The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null).
Response: **The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The intent of the SDT is to uphold the directive from Paragraph 381 of FERC Order 706 which clarifies that the senior manager is not a user, owner, or operator of the Bulk Power System who is personally subject to civil penalties pursuant to Section 215 of FPA. The SDT believes that delegation should be addressed in the CIP standards in order to ensure that the appropriate governance structure is considered by the Responsible Entity.** **We have received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002**		

Organization	Yes or No	Question 2 Comment
in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Dynegy	No	Agree with proposed modifications except recommend moving CIP-003, R2 into the CIP-002 Standard (see comment on Item #1).
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Northern Indiana Public Service Company	No	As stated in question 1 I believe the revised applicability in CIP-003-2 section 4.2.3 is oddly placed as an entity could read CIP-002-2 in entirety and feel that the resulting null asset list excludes the entity from any other CIP standards. If a single requirement also applies to an entity that has a resulting null list, I believe it is better to call out the additional requirement within CIP-002-2 R4 rather than adding revised applicability language to CIP-003-2.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency	No	IMEA agrees with the intent of the proposed modifications, but recommends they be incorporated into CIP-002-1 (instead of CIP-003-1) modifications for clarification of applicability regardless of Critical

Organization	Yes or No	Question 2 Comment
		Cyber Asset identification.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario Power Generation		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	No	With respect to individual bullet points: (1) We find this question confusing. We interpret Applicability as written to mean that those Responsible Entities that have determined that they have no Critical Cyber Assets need only to meet R2 of CIP-003. The question as posted here seems to suggest that R2 of CIP-003 only applies to these Responsible Entities, but NOT to those other Responsible Entities that have identified that they have Critical Cyber Assets. Please clarify. Currently, only CIP-002 is applicable to entities without Critical Assets. Thus, the recommended modification to CIP-003 would be insufficient for accomplishing the intent of the change. One solution might be to move the Senior Manager appointment requirement from CIP-003 R2 to CIP-002 (as suggested under Q1), or incorporate the requirement for a Senior Manager appointment by

Organization	Yes or No	Question 2 Comment
		reference within CIP-002. (2) Agreed, and this is consistent with our comments on CIP-002, above. (3) Agreed (4) Agreed (5) Agreed
Response: **To clarify, the question refers to the addition of a requirement for entities with no Critical Cyber Assets, not the exclusive application of CIP-003-2 R2 to entities with no Critical Cyber Assets. All Responsible Entities, regardless of their ownership of critical assets, are required to meet CIP-003-2 R2.** **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ameren	Yes	None.
Response: **Thank you for your comment.**		
Consumers Energy Company	Yes	
Xcel Energy	No	It appears as though R3.2 could be interpreted to require compensating measures, once the phrase "or a statement accepting risk" is eliminated. We would like clarification if this was the intent.
Response: **The phrase “any compensating measures” is not intended to require compensating measures. As an Entity is free to develop a Cyber Security Policy which exceeds the minimum requirements of CIP-002-2 through CIP-009-2, there exists the case where an Entity may take exception to its Cyber Security Policy, but still meet all of the CIP requirements. Consequently, the SDT concluded that it was overreaching to require compensating measures for all exceptions to the Cyber Security Policy at this time.**		

Organization	Yes or No	Question 2 Comment
ISO New England Inc	No	1) In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundent and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice. 2) We recommend moving CIP-003 R2 into the CIP-002 Standard. Therefore the change to APPLICABILITY 4.2.3 would not be necessary. 3) We take exceptiopn to the inclusion of the words "single" and "authority." These inclusions present a specific example where the CIP Standards are too prescriptive in that they seek to regulate company's internal management, as opposed to regulating performance. This modification is inappropriate and potentially outside NERC's legislative mandate. The drafting team must explain what it intends by adding the word "authority" to the word "responsibility." Second, if "authority" is given a meaning of having the power to ensure that capital resources are expended to achieve the objectives laid out in the Standard, we have questions about how NERC can propose regulating how companies manage their budgets. Some companies budgets must be approved by their Boards, and some companies' budgets must be approved by FERC. 4) We support the change to R2.1 5) We request clarification of CIP-003 R2.3. Would very short term delegations (less than 30 days) for vacation and out-of-office travel need same level of recording and Senior Manager approval. 6) In this Standard and throughout several other CIP Standards, the lead focus statement in the Measures is re-stated redundantly throughout each of the bulleted Measure statements. Please clean-up such text.

Response:

1) The addition of the "implement" language was in response to a determination in the FERC Order. [Please refer to FERC Order 706 Paragraph 75.]

2) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.

3) The SDT believes that R2.3 provides Responsible Entities the flexibility to meet the leadership requirements without prescribing organizational changes.

Organization	Yes or No	Question 2 Comment
4) Thank you for your comment. **5) There is no adjustment of the requirement based upon longevity of absence.** **6) This modification was done in order to be in line with the structure of other ERO standards.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	No	We believe that R3.2 should be revised to require an analysis of risk, in order to provide understanding of what the compensating measures are achieving. Suggested language is as follows: "Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary, any compensating measures, and analysis of residual risk."
Response: **The SDT does not intend to prescribe an analysis of risk for all exceptions. Please readdress this issue during the phase 2 comment period.**		
Brazos Electric Power Cooperative, Inc.	No	Under the Applicability section it makes no sense for a Responsible Entity to have to comply with CIP003 R2 when there are no CCAs. This should be deleted.
Response: **The intent of the application of CIP-003-2 R2 to Responsible Entities with no Critical Cyber Assets is to ensure that the appropriate individual approves the null list of Critical Cyber Assets.**		
Progress Energy	Yes	
Standards Review Committee of ISO/RTO Council	Yes No	(1) We are confused by the question asked here. We interpret Applicability as written to mean that those Responsible Entities that have determined that they have no Critical Cyber Assets need only to meet R2 of CIP-003. The question as posted here seems to suggest that R2 of CIP-003 only applies to these Responsible Entities, but NOT to those other Responsible Entities that have identified that they have Critical Cyber Assets. Please clarify. Currently, only CIP-002 is applicable to entities without Critical Assets. Thus, the recommended modification to CIP-003 would be insufficient for accomplishing the intent of the change. One solution

Organization	Yes or No	Question 2 Comment
		might be to move the Senior Manager appointment requirement from CIP-003 R2 to CIP-002 (as suggested under Q1), or incorporate the requirement for a Senior Manager appointment by reference within CIP-002. Specific to R2, notwithstanding the above recommendation to move it to CIP-002, we have concerns with the inclusion of the words "single" and "authority." These inclusions present a specific example where the CIP Standards are overly prescriptive in that they seek to regulate company's internal management, as opposed to regulating performance. This modification is inappropriate, unnecessary and outside NERC's legislative mandate. The drafting team must explain what it intends by adding the word "authority" to the word "responsibility." Second, if "authority" is given a meaning of having the power to ensure that capital resources are expended to achieve the objectives laid out in the Standard, we have questions about how NERC can propose regulating how companies manage their budgets. Some companies budgets must be approved by their Boards, and some companies' budgets must be approved by FERC. (2) Agreed, and this is consistent with our comments on CIP-002, above. (3) Agreed (4) Agreed (5) Agreed
Response: **To clarify, the question refers to the addition of a requirement for entities with no Critical Cyber Assets, not the exclusive application of CIP-003-2 R2 to entities with no Critical Cyber Assets. All Responsible Entities, regardless of their ownership of critical assets, are required to meet CIP-003-2 R2.** **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
KEMA	No	Agree with all modifications, but strongly suggest rather than deleting the phrase "or a statement accepting risk" rewording it instead. Any time compensating measures are used instead of complying with established policy or standards, some residual risk is always involved, which must be acknowledged and accepted by executive management. Use wording similar to: "...any compensating measures with executive management accepting any residual security risks." This will also force

Organization	Yes or No	Question 2 Comment
		individuals to develop compensating measures with adequate coverage.
Response: **The SDT will consider a Risk Management Framework as defined by NIST during future phases of modifications as directed by FERC Order 706. In addition, FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process. [Please refer to FERC 706, Paragraph 151]**		
Austin Energy	Yes	
Kansas City Power & Light	No	In CIP-003 R2, internal political difficulties are created by requiring the designated senior manager to have the authority to implement the security program. Many medium to large utilities have IT departments separate from their operations or compliance departments. In order to find a manager of sufficient direct line authority, you have moved to a level within the organization where the manager will either not have the appropriate level of knowledge to review compliance actions or will not have sufficient time to dedicate to the task. Either way, all that will occur will be a perfunctory signature on the compliance documentation which defeats multiple goals of the program. I believe most utilities will want to comply with the spirit of this provision, but the proposed phrasing will make doing so more difficult.
Response: **The senior manager is held responsible to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation needs to be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity.** **The responsibilities of the senior manager may be delegated with the exception of approving (1) the Cyber Security Policy required by CIP-003, Requirement R1; (2) the Risk-based Assessment Methodology required by CIP-002, Requirement R1, and (3) the technical feasibility exceptions. For those instances where delegation is not permitted or not granted, the senior manager would reasonably be expected to seek the advice of technically qualified staff before giving approval.**		
San Diego Gas and Electric Co.	Yes	

3. The The CSO706 SDT is proposing the following modifications to **CIP-004-1**:
   - In R1 and R2, clarify the requirement to implement security awareness and annual cyber security training programs.
   - Revise R2.1 to train personnel prior to granting access (per FERC Order, paragraph 431).
   - Revise R3 to complete a personnel risk assessment prior to granting access (per FERC Order, paragraph 443).
   - In Requirements R2.1 and R3, the SDT adopted the FERC Order 706 language, "except in specified circumstances such as an emergency," to address unusual events that demand urgent action before the personnel risk assessment can be completed.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 3 Comment
Detroit Edison Company	No	The language "except in specified circumstances such as emergency." introduces ambiguity into this requirement. What would other circumstances be? Is each Responsible Entity allowed to define this on their own? Paragraph 443 of FERC order 706 directs the SDT to provide guidance on defining emergencies. "The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency. We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process."
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances**		
PacifiCorp	Yes	
FirstEnergy Corp	No	Regarding R2.1 and R3, we believe that the phrase "specified circumstances such as an emergency" is ambiguous. It is not clear what would constitute acceptable "specified circumstances" other than an emergency situation. This phrase should be replaced with simply "emergency situations", which would also be consistant with language in other CIP requirements such as in CIP-003 R1.1.

Organization	Yes or No	Question 3 Comment
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.**		
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	Yes	
WECC Relibaility Coordination	No	do not agree with R1.2 that personnel need to be trained before they are granted access. Training in this area is extensive and we feel the 90 day window allows appropriate training to take place along with our employee orientation.
Response: **It has been identified in FERC Order 706 and the SDT agrees that the requisite training shall be completed prior to granting unescorted access. Providing escorted access is permitted prior to the requisite training being completed. Granting unescorted access is permitted for specified circumstances such as an emergency prior to the requisite training being completed. The responsible entity shall define their own specified circumstances and document them within their cyber security training program or cyber security policy.**		
Southern Company	Yes	CIP-004 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-004 Section D - Compliance: 1.4.2 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-004 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure.**		

Organization	Yes or No	Question 3 Comment
Paragraphs 404 and 405). **1.4.2 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. The new language within R2.1 allows for an exception in specific circumstances. What are specified circumstances? And, if these specific circumstances occur do the individuals ever have to take the training? - The prior requirement was within ninety calendar days. 2. An additional crossover requirement exists leading to confusion. CIP-006-2 R3 now states cyber assets residing in a PSP; however the language now in CIP-004-2 does not require access to Cyber Assets to undergo training, awareness and PRAs. We recommend providing further clarification around this requirement.— General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 3. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: **1. This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.** **2. If personnel roles and responsibilities require access after the specified circumstance, then training must be completed**		

Organization	Yes or No	Question 3 Comment
according to CIP-004. Personnel can be granted such access as long as a personnel risk assessment has been conducted according to the requirements in R3, and the minimum training has been conducted according to personnel roles and responsibilities according to the requirements in R2. **3. The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence.** **The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.** **The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	CIP-003 requires "including provision for emergency situations" in the Entity's cyber security policy. This "emergency" is referenced in CIP-004 R2.1 and R3. Nowhere in the standards is any requirement or more specific guidance provided in what should be addressed in these provisions: e.g. description of what it is and who declares it, start and end conditions, documentation requirements: is it left to the entity to set its own parameters on how and what to declare as an emergency?
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.**		

Organization	Yes or No	Question 3 Comment
Southern California Edison Company	Yes	
Tampa Electric Company	No	Requirement R3 The proposed changes would result in the language: "....A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency."(removing within 30 days of being granted access). This would leave the standard open to the interpretation that as long as an assessment is no older than 7 years old, then this risk assessment is "prior" to the personnel begin granted access. Tampa Electric is unsure if this is the intention of the language change. If this is not the intenct, then the wording should be clarified. Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: **As stated in R3, personnel can be granted such access as long as the personnel risk assessment has been conducted within the last seven years. CIP-003-2 Requirement R3 includes the identification and approval of exceptions to the corporate Cyber Security Policy.Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Suggest rewording Requirement R2.1 as follows: "This program will ensure that all personnel requiring access to Critical Cyber Assets," for clarity.
Response: **1) NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific**		

Organization	Yes or No	Question 3 Comment
directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates	Yes	We agree with the proposed modifications especially with the phrase "except in specified circumstances such as an emergency". Similar to CIP-002-2, D. Compliance, Section 1.5, should CIP-004-2, D. Compliance, Section 1.5 say "None"?
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
United Illuminating Company	Yes	
Deloitte & Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal training and awareness program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	Yes	

Organization	Yes or No	Question 3 Comment
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation		
Applied Control Solutions, LLC	No	Training needs to be specifically control system cyber security training
Response: **R2.2 defines minimum required items which are Critical Cyber Asset specific.**		
US Bureau of Reclamation	No	Requirement R2 needs to more specifically distinguish between access types and required training. Individuals with physical access may only need general security awareness training, whereas those with physical and logical access may require specific role-based training. The requirement, as written, addresses proper use of cyber assets, physical and logical access controls, proper handling of information, etc., in what appears to be an all-inclusive manner. Some of these training requirements would appear to be unnecessary for an individual who may only need limited physical access and the requirement should support this. The requirement does not recognize that Entities may have a more rigorous background check process which takes longer than the abbreviated process described in the standard. While describing the minimum helps to clarify what is needed, the standard should allow Entities that have more rigorous requirements longer time frames to implement the background checks. In most cases the background checks timeframes are not within the control of the Entity. In addition the standard would hamper the ability of existing experienced staff who have passed a more exhaustive check from operating thereby defeating the value to reliability. Can the requirement, R3, be structured in such a manner as to support access following initial screening in situations where full investigations may take a significant period of time? As an example, a national security check resulting in a clearance may take an extended period of time, limiting an organization's ability to utilize an employee - even in a decreased sensitivity role - while awaiting results. If the employee is allowed access - even limited - following a preliminary check (through local/national law enforcement agencies), would this meet the intent of the requirements while awaiting the results of a full and more comprehensive investigation? Further, is there a means, within the present requirements, to address the temporary "grandfathering" of

Organization	Yes or No	Question 3 Comment
		individuals who have access today while they are undergoing investigations? Without such an allowance, staff availability, during investigation activities, could be severely limited.
Response: **Personnel can be granted such access as long as a personnel risk assessment has been conducted according to the requirements in R3, and the minimum training has been conducted according to personnel roles and responsibilities according to the requirements in R2. A national security investigation contains elements beyond the scope of R3, which are not necessary to meet R3.As stated in R3, personnel can be granted access as long as the personnel risk assessment has been conducted within the last seven years. If a personnel risk assessment has not been conducted within the last seven years, it must be completed before the individual can be granted access.**		
Orange and Rockland Utilities Inc.	No	CIP-003 requires "including provision for emergency situations" in the Entity's cyber security policy. This "emergency" is referenced in CIP-004 R2.1 and R3. Nowhere in the standards is any requirement or more specific guidance provided in what should be addressed in these provisions: e.g. description of what it is and who declares it, start and end conditions, documentation requirements: is it left to the entity to set its own parameters on how and what to declare as an emergency?
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.**		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator	No	The term "specified circumstances" implies that a set of circumstances is specified somewhere. Where is this list and who will decide what comprises it? Suggest that this list be clarified.
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.**		
Dynegy	Yes	

Organization	Yes or No	Question 3 Comment
Northern Indiana Public Service Company	No	Clarification regarding the definition of specified circumstances and emergency conditions is needed. Additionally, language needs to be added to clarify what steps need to be taken if an emergency occurs and access is granted. As the draft reads, an entity could declare an emergency, grant access, and document the emergency condition. There is no language directing follow up action that would ever require the responsible entity to perform training or a PRA of the individual that was granted access under the emergency condition. Depending on the direction provided from the drafting team in regards to what would consist of an emergency, the removal of the 30-90 day after the fact language may create significant concern in regards to bargaining unit operations and service personnel. Secondly, I have a comment regarding the additional clarifying language that was added to CIP004-2 R1 to indicate applicability to critical cyber assets. I understand that this language was added to provide uniformity in scope between CIP-004-2 R1, R2, and all of the respective sub-requirements. I have a concern regarding the absence of the CCA language in CIP-004-2 R3. I feel R3 should be modified to include similar CCA language to provide uniformity with R1, R2 and the R3 sub-requirements.
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.** **If personnel roles and responsibilities require access after the specified circumstance, then training and a personnel risk assessment must be conducted according to CIP-004.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation		

Organization	Yes or No	Question 3 Comment
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	No	The elimination of the 30 day temporary access time will have a significant "operational" impact to fill personnel positions in a timely manner within protected areas. Without the 30 day temporary access criteria, personnel will not be allowed "unescorted" access into a facility until the candidate has completed training and a background check is completed, reviewed and returned with a positive and acceptable response. Additionally, mandating that another employee watch or "escort" the new candidate all the time during their shift is both a nuisance and a possible safety hazard. It is important to note that this proposed change is a "180 degree conceptual change" from what was a noticeable and unwavering stance that most companies took when the original CIP standards were implemented. Not being able to shift personnel around from one area of the company to the protected-area assignments (when personnel are re-assigned) immediately, places an unnecessary burden on both areas of the company. When comparing the proposed change to the current process, the benefits gained by the elimination of the 30-day temporary access window clearly don't outweigh what is already a solid and workable solution.
Response: **It has been identified in FERC Order 706 and the SDT agrees that the personnel risk assessment and requisite training shall be completed prior to granting unescorted access. Providing escorted access is permitted prior to the personnel risk assessment and requisite training being completed. Granting unescorted access is permitted for specified circumstances such as an emergency prior to the personnel risk assessment and requisite training being completed. The responsible entity shall define their own specified circumstances and document them within their cyber security training program, personnel risk assessment program, or**		

Organization	Yes or No	Question 3 Comment
cyber security policy.		
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1 - In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundent and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice.
Response: **The word 'implement' was included per FERC Order 706 Paragraph 75 to remove any doubt that a particular process/procedure/program could be only designed, developed, documented but not implemented. This was a result of previous questions around implementation from Industry. It is added for clarity and completeness**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
Progress Energy	Yes	CIP004R2 – The cyber security training program shall be annually reviewed and updated as necessary – Please provide clarification, does updated as necessary mean updates only need to occur annually during the annual review period?
Response: **The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.**		

Organization	Yes or No	Question 3 Comment
Standards Review Committee of ISO/RTO Council	No	In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundant and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice.
Response: **The word 'implement' was included per FERC Order 706 Paragraph 75 to remove any doubt that a particular process/procedure/program could be only designed, developed, documented but not implemented. This was a result of previous questions around implementation from Industry. It is added for clarity and completeness.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	No	To help clarify training requirements for different users and access levels, SDG&E would like to see language added to CIP-004-1 R2.2 stating that training should be appropriate to user duties, functions, experience, and access level. Information concerning vulnerabilities should be revealed on a need to know basis and not universally.
Response: **Given the limited scope and timeline for Phase 1, please readdress this issue during the Phase 2 comment period.**		

4. The CSO706 SDT is proposing the following modifications to **CIP-005-1**:

   - In R1.5, clarify the requirement to safeguard Cyber Assets used in the control or monitoring of Electronic Security Perimeter.
   - The term "implement" was added to CIP-005-1 Requirement R2.3 to clarify that the procedure for securing dial-up access to the Electronic Security Perimeter must be both maintained and implemented.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 4 Comment
Detroit Edison Company	Yes	
PacifiCorp	No	Yes to the second bullet. No to the first bullet and other points.R1.1 - It is unclear what is meant by "externally connected". Does "connectivity" refer to logical or physical connectivity? Is "external" a reference to the ESP in question, or to the entity? Is it a reference to layer 3 (and above)? PacifiCorp recommends some clarifying language similar to the following: • Any device accessible via routable protocol (layer 3) from outside the ESP is an access point unless such traffic is already passing through and controlled (layer 3) by another CIP005 compliant access point. • Additionally, any device serving as an endpoint of an encrypted and/or encapsulated layer 3 (and above) tunnel (IPSEC, GRE, SSL-VPN, SSH, CIPE, etc..) which provides remote network connectivity to the ESP network and not merely application access to the host itself, and where the other endpoint is outside the ESP, is also an access point.? • Externally connected also includes devices accessible via modem or any form of wireless access point providing network connectivity to other devices within the ESP." • Externally connected does not include encrypted communication links where the end points are within the ESP.R1.3 - This should be eliminated. By definition,

Organization	Yes or No	Question 4 Comment
		communication links between discrete ESPs are “out of scope” (CIP-005-2 4.2.2) Additionally, where such links are using routable protocols, the termination point would be a “communication end point” and thus covered by R1.1. This section provides no additional value.R1.5 references to CIP005.R2 and CIP005.R3 should be removed as these are not applicable to the access control and monitoring equipment which are not "Access points". Additionally, the proper security practices for these devices are covered under CIP007 R2-R9.R1.5 (continued) - The access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as mobile devices. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. PacifiCorp believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting mobile devices used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.PAC proposes the following language: R3. Protection of Electronic Access Control Systems - Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for mobile devices, for which the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.
Response: **These types of issues will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns have not been addressed.**		
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	Comment: On CIP-005, R1.5, the access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as client-server applications. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. For example, we cannot place laptops used by technicians inside a physical security perimeter. MidAmerican believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.MEC proposes the following language: CIP-006 R3. Protection of Electronic Access Control Systems - Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong

Organization	Yes or No	Question 4 Comment
		procedural or technical controls to ensure authenticity of the accessing party.
Response: **The scope of the modification is only to include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Northeast Power Coordinating Council	No	"Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently.
Response: **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	CIP-005 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-005 Section D - Compliance: 1.4.2- Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-005 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a**		

Organization	Yes or No	Question 4 Comment
vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405). **1.4.2 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. It is very important to define monitoring in the new context. Originally the cyber assets had to be used for the dual purpose of access control and monitoring. Now, simply a monitoring device is considered a cyber asset under this new language. We ask for an additional clarification around to what extent monitoring is covered, for example: a. The original monitoring cyber asset (device a) b. 2. The cyber asset receiving alerts from the original device (device b) c. 3. The cyber asset forwarding the alerts (device c) d. 4. The cyber asset receiving the alerts (device d)The current language could be interpreted in a way that a blackberry receiving alerts is "monitoring" the ESP. General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Organization	Yes or No	Question 4 Comment
Response: **1) The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **3) The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence.** **The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.** **The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	No	The revision to CIP-005-2 R1.5 referenced only CIP-006-2 R3. CIP-003 R3 requires that the organization identify the Physical Security Perimeter. In the original CIP-005-1 R1.5, the physical protections had to meet CIP-006-1 R2 and R3 which are now renumbered R4 and R5 in CIP-006-2. This represents a major revision and a much less robust security in the physical protection requirements

Organization	Yes or No	Question 4 Comment
		for cyber assets used for access control or monitoring of the Electronic Security Perimeter. To retain the original intent of CIP-005-1 R1.5, the requirement must include a reference to CIP-006-2 R3, R4, and R5.
Response: **CIP-006-R3 requires placing the devices of CIP-005-2 R1.5 within a Physical Security Perimeter. Once a device is within a Physical Security Perimeter, physical control is automatically established, making these inclusions redundant.**		
Consolidated Edison Company of New York, Inc.	No	"Dated" is used only in the Measures (M1, M2, M3, M4, M5). The corresponding requirements do not state a requirement for a date: adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently
Response: **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
Southern California Edison Company	Yes	Request clarification on the difference between "process" and "procedure."
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Tampa Electric Company	No	In R1.5, the change from "and" to "and/or" could bring unintended devices into scope of this standard. The change should be clarified to say "access control of and/or monitoring access to of the Electronic Security Perimeter(s)." Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."

Organization	Yes or No	Question 4 Comment
Response: **The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Situations where standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The TFE process will address the requirements for documenting, approving, and remediating the exception.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	No	On CIP-005, R1.5, the access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as client-server applications. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. For example, we cannot place laptops used by technicians inside a physical security perimeter. The MRO NSRS believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.The MRO NSRS proposes the following language: CIP-006 R3. Protection of Electronic Access Control Systems? Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.

Organization	Yes or No	Question 4 Comment
Response: **The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Pepco Holdings, Inc - Affiliates	Yes	
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e., a documentation of a formal dial-up security program and procedure that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	Yes	We support all comments noted for CIP005 in this section with the recommendation to move the word implement before maintain in R2.3 so the sentence reads ?implement and maintain.? Reason for the recommendation is a control must be implemented before it can be maintained
Response: **The SDT will make the appropriate change in R2.3 from “maintain and implement” to “implement and maintain”.**		
Old Dominion Electric Cooperative		

Organization	Yes or No	Question 4 Comment
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	The standard should be worded to be applicable for existing dial-up access or if dial-up access is added.
Response: **The requirement applies to all dial-up access, both existing and future.**		
Orange and Rockland Utilities Inc.	No	"Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently
Response: **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator	Yes	
Dynegy	Yes	
Northern Indiana Public	No	I would request a clarification on scope and depth of the devices to be included in the access control

Organization	Yes or No	Question 4 Comment
Service Company		and/or monitoring. The previous language would have limited the devices to those that performed access control and monitoring of the ESP (traditional Firewalls, routers with ACL's, any IPS devices, VPN endpoints, etc.). The new language provided in the draft under CIP-005-2 R1.5 modifies the scope to include cyber assets used in the access control and/or monitoring of the ESP. I am concerned with the depth of devices involved in the monitoring chain that have no relevance on access control, but are an active component in the monitoring of the ESP. Specifically: log correlation servers, SNMP trap servers, SMTP relay servers for notification, pagers, blackberry's, enterprise email servers, backup and recovery servers for these extended devices, etc.. In the current draft it is unclear whether the device performing the monitoring is the only device that is subject to the requirements specified in CIP-005-2 R1.5 or if all devices involved in monitoring are subject to those requirements specified in CIP-005-2 R1.5. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets used in the monitoring of the ESP.
Response: **The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	R1.5 creates issues where an entity may be using a third party to remotely monitor and administer Cyber Assets used in the control or monitoring of the ESP. The new requirement will require the entity to police the physical security measures of any such third party to a degree not required for third parties who may support CCAs within the ESP. OPG suggests that the requirements for Cyber Assets used in the access control and / or monitoring of the ESP require protections to the same standards as those

Organization	Yes or No	Question 4 Comment
		which are used to access CCAs
Response: **Requirements apply regardless of who performs the functions.**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. 2) R1 refers to documentation while M1 uses documents. Recommend using documentation consistently.

Organization	Yes or No	Question 4 Comment
Response: **1) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.** **2) The text will be changed to read "documentation".** **The SDT has received numerous comments related to wording preferences. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
Progress Energy	Yes	
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	

Organization	Yes or No	Question 4 Comment
San Diego Gas and Electric Co.	Yes	

5. The CSO706 SDT is proposing the following modifications to **CIP-006-1**:

- Clarify Requirement R1 that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. CIP-006-1 Requirements R1.1 through R1.7 and R1.9 were revised to clarify the elements that, at a minimum, must be addressed in the physical security plan.
- The SDT added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2.
- The SDT added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter.
- Subsequent Requirements were renumbered and references were appropriately revised. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to lists of options consistent with the intent of the requirements.
- The SDT revised the Measures to add “implementation” to Measure M1 documentation elements for Requirement R1, added Measure M2 to document the protection of physical access control systems, added Measure M3 to document the protection of electronic access control systems, and renumbered subsequent Measures and references to Requirements. The SDT also added failure to implement the security plan as Level 4 non-compliance.

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 5 Comment
Detroit Edison Company	No	CIP-006-2 R1.4 references "physical access controls as described in Requirement R3". R1.4 should reference Requirement R4 since the requirements were renumbered and Physical Access Controls is now R4.CIP-006-2 Introduction, 3. Purpose, it should read something like, ?. . . . . to ensure the implementation and continued maintenance of a physical . . . . . ? This program is not only being implemented, but will also be maintained going forward. (i.e. ? does not make sense to implement a program and do nothing else)CIP-006-2 Introduction, 4.2 The following are exempt from Standard CIP-006-2, in addition to listing the exemptions to NERC Standard CIP-006, they may also want to comment

Organization	Yes or No	Question 5 Comment
		on potentially overlapping security requirements for facilities which are also regulated under the Maritime Transportation Security Act (33 CFR 101/105) and the Chemical Facility Anti-Terrorism Standards. (6 CFR 27)CIP-006-2 R2 Protection of Physical Access Control Systems, sub-requirements R2.1 & R2.2. R2.1 is ambiguous in that it states, "Be protected from unauthorized physical access," yet it does not explain how this is to be accomplished. R2.2 defines the protective measures to be utilized? R4 and R5, Physical Access Controls and Monitoring Physical Access. It appears they want to grant the responsible entity flexibility in R2.1, but then it is limited by R2.2. These two sub-requirements should be combined into one to avoid confusion.
Response: **The Drafting team agrees that R1.4 should reference R4 and not R3. This change will be implemented. With regard to inclusion of maintenance within the Purpose of the requirement, the drafting team agrees that this could add clarity however for consistency we would need to review how this would impact the purpose statements of the remaining CIP standards hence this will be addressed in Phase 2. The issue of conflicting regulatory authorities will be brought before NERC for discussion. Relating to protection of Physical Access Control Systems, reliability standards only prescribe "What" and not "How". These types of issues will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
PacifiCorp	No	No for the third bullet (R3) (See comment on CIP-005-2). Yes for remaining bullets.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	See comment for question 5
Response: **The scope of the modification is only to include devices that perform access control and/or monitoring as identified in CIP-005 R2**		

Organization	Yes or No	Question 5 Comment
and R3 and not those devices that are receiving alerts. **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Northeast Power Coordinating Council	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points". 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous", and that it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the entity's change process for any".
Response: **1) Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2) The drafting team agrees and will implement this change.** **3) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).** **4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	CIP-006 R1.1 - Change to the last sentence should be clarifed that it applies to Critical Cyber Assets and not Critical Assets.

Organization	Yes or No	Question 5 Comment
		R1.4 makes reference to "Requirement 3", but the correct reference in the new standard should now be "Requirement 5". CIP-006 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-006 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-006 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: **Within CIP-006 R1.1, the requirement now reads "to such Cyber Assets". The Drafting team agrees that the R1.4 reference is incorrect. The SDT points out that the correct reference is R4 and not R5.** **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. The redlining appears to be inaccurate. For example R2 in CIP-006-1 is now R4 in CIP-006-2. This modification is very important to note as compliance monitoring systems may have been defined to key on the requirement field.2. CIP-006-2 R4/R5/R6 now use bullets instead of numbered identifiers for the individual physical access methods. A unique identifier should be selected to identify these bulleted

Organization	Yes or No	Question 5 Comment
		items.3. R3 requires cyber assets used in the access control and/or monitoring of the ESP to be in a PSP. Please see our comments in Question 4 (CIP-005-2) pertaining to the extent of what assets need to be in a PSP (device a / b / c / d). --General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Response:

1) **The drafting team agrees that not all of the changes are clearly identified. The posted version (the one that was commented on) is the official version, and while the drafting team did renumber some of the requirements, these are consistent across the reliability standards.**

2) **The changes that made individual sub-requirements into bullets were made to correct an original error, since requirements cannot be levied upon an item that may not be implemented.**

3) **CIP-006-R3 requires placing the devices of CIP-005-2 R1.5 within a Physical Security Perimeter. Once a device is within a Physical Security Perimeter, physical control is automatically established, making these inclusions redundant. Relating to not including all of the changes within the questions, the questions were meant to only address substantive changes to the standards.**

General: The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence.

The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.

The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.

Organization	Yes or No	Question 5 Comment
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	No	While the majority of the revisions to R1 do provide clarity, the revision to Requirement R1.1 is less clear than the previous version and represents a change to the requirement. In the previous version, R1.1 requires that the Physical Security Plan address "Processes to ensure and document that" all Cyber Assets within an Electronic Security Perimeter reside within an identified Physical Security Perimeter consisting of a six-wall border. With this new revision, the Physical Security Plan shall address all Cyber Assets within an Electronic Security Perimeter. Address cyber assets how? There is no longer any requirement to describe the process the organization uses to ensure that cyber assets reside within an identified Physical Security Perimeter. Is the intent of this revision to clarify that a Physical Security Plan must simply exist and address identified Physical Security Perimeters protecting Cyber Assets within an Electronic Security Perimeter? There is no requirement for Physical Security Plans for cyber assets used for access control and/or monitoring of Physical Security Perimeters or Electronic Security Perimeters. If the intent of Phase 1 changes to R1 are simply to provide clarity, then recommend retaining the original R1.1 text from the previous version and make changes to R1.1 in a later phase of Project 2008-06 - Cyber Security Order 706.
Response: **Requirement 1 identifies what must be within the Physical Security Plan, and Requirement 1.1 identifies that all cyber assets within an ESP must be within a Physical Security Perimeter, (i.e, the plan must address ensuring that all cyber assets within an ESP are within a PSP). Relating to exclusion of cyber assets used for access control and/or monitoring from the Physical Security Plan, the SDT refers you to Requirements 1.2 and 1.3.**		
Consolidated Edison Company of New York, Inc.	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous," it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any": a change generally includes more processes than just the change, e.g. acceptance period, required internal approvals,

Organization	Yes or No	Question 5 Comment
		"as built" regulatory approvals.
Response: **1) Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2) The drafting team agrees and will implement this change.** **3) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).** **4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Southern California Edison Company	No	For R1.8 Annual review and approval - we interpret it as the Senior Manager or delegate reviews and approves the physical security plan annually. For consistency with R2, suggest re-wording R3 to: "Protection of Electronic Access Control Systems - Cyber Assets that authorize and/or log access to the Electronic Security Perimeter (s) shall reside within an identified Physical Security Perimeter." Delete R2.1.
Response: **The drafting team feels that since Requirement 1.8 is a subrequirement of Requirement 1, it is appropriate to interpret that the annual review would be signed off by the senior manager or delegate as identified in Requirement 1.** **For your additional comments, these types of issues will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
Tampa Electric Company	No	Requirement 1.3: Remove "processes" from the wording to be consistent with the other changes in CIP006 Requirement 1 and eliminate the redundancy of having "processes" and "procedures" in same statement. Processes are included in the procedures. Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the

Organization	Yes or No	Question 5 Comment
		standard: “Duly authorized exceptions will not result in non-compliance.”
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that “duly authorized exceptions will not result in non-compliance” within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Requirement R1.4, it is not clear what is intended by the phrase "response to loss." . 3) Requirement R1.4 should reference R4 rather than R3. 4) Suggest standardizing the language used in R4, R5 and R6. (R4 refers to security personnel; R5, second bullet, to authorized personnel; R6, third bullet, to security or other authorized personnel.)
Response: **1) NERC and Regional Entity are defined in NERC’s corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **2) Due to the limited scope and timeline for Phase 1, issues such as “response to loss” will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns have not been addressed.** **3) The drafting team agrees with the correction of Requirement 1.4, and will implement this.** **4) Standardizing language will additionally be addressed in Phase 2.**		
PPL Corporation	No	Recommend a correction to R1.4 which references R3. We believe this is now R4.

Organization	Yes or No	Question 5 Comment
Response: **The drafting team agrees with the correction of Requirement 1.4, and will implement this.**		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.The MRO NSRS proposes the following language:CIP-006 R3. Protection of Electronic Access Control Systems ? Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party. The MRO NSRS agrees with the remaining changes in CIP-006-2.
Response: **You bring up a good point of clarification. The intent of the modification was to clarify that a device that performs either function must be included. However an unintended consequence of this change was to add ambiguity as to what constitutes a monitoring device. The intent is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Pepco Holdings, Inc - Affiliates		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal physical security program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).

Organization	Yes or No	Question 5 Comment
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	Yes	Recommendation to increase the timeframe in R1.7 to update the physical security plan to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation. We support all the other comments noted for CIP006 in this section with the recommendation to move the word implement before maintain in R1 so the sentence reads “create, implement and maintain.” Reason for the recommendation is a control must be implemented before it can be maintained. .
Response: **Thank you for your comments. They will be considered in future phases of these standards.** **Revising the order of “create, implement, and maintain” is accepted.**		
Old Dominion Electric Cooperative		
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	The requirement that the Physical Security plan be approved by a single senior manager is not appropriate. It should be sufficient to require that the entity have a management approved plan. As stated before, submissions from the regional entities in geographically diverse entities pass through and are certified by the entity's compliance POC and represent an official entity position and commitment to action. To require more adds an unnecessary organizational and administrative burden.

Organization	Yes or No	Question 5 Comment
Response: **The requirement specifically provides for the Senior Manager or delegate(s) to approve the plan, thereby providing enough flexibility while maintaining a specific chain of authority.**		
Orange and Rockland Utilities Inc.	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous," it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any"
Response: **1) Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2) The drafting team agrees and will implement this change.** **3) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).** **4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CenterPoint Energy	No	An additional modification that was proposed by the SDT in R1.7 reduced the amount of time allowed for making changes and updates to the physical security plan from 90 days to 30 days. CenterPoint Energy strongly disagrees with this change. Furthermore, the Commission did not direct this change in Order 706 or Order 706A. CenterPoint Energy believes 30 days is too constraining and unwarranted, and that 90 days should be retained. If the SDT moves forward with the proposed reduction in time, CenterPoint Energy proposes 60 days to allow for a complete review of any physical security plan changes.

Organization	Yes or No	Question 5 Comment
Response: **The drafting team understands your concerns, however for consistency across all CIP standards, short term implementations were reduced from 90 days to 30 days.**		
Manitoba Hydro	No	The wording in R2 should be: "Cyber Assets used in the access control and/or monitoring and/or logging access to the Physical Security Perimeter(s)", to reflect similar wording in R3, and to include other devices or systems used in access control, such as authentication systems.
Response: **Issues such as clarifying the difference between logging and monitoring will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns were not addressed.**		
Alberta Electric System Operator	Yes	R1.1 is missing the word, "critical" for Cyber Assets. There is no need to have a requirement for assets that are not critical.
Response: **Requirement 1.1 specifically addresses Cyber Assets and not the subset of Critical Cyber Assets. Any device that is within the same Electronic Security Perimeter as a Critical Cyber Asset must be within a Physical Security Perimeter and hence must be addressed within the Physical Security plan.**		
Dynegy	No	1. Recommend changing R1.2 to require identification of all "physical" access points. 2. Correct R1.4 to reference R4 instead of R3. 3. Eliminate "continuous" from R1.6. This term is not auditable.
Response: **1. Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2. The drafting team agrees and will implement this change.** **3. The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).**		

Organization	Yes or No	Question 5 Comment
Northern Indiana Public Service Company	No	In future drafts I would encourage the drafting team to enable track changes on the modifications to the requirements numbers as well as the text. Modifications to requirement numbers, especially in CIP-006-2 were not consistently red-lined to display where the content was formerly referenced in the existing CIP-006-1. Regarding CIP-006-2 R2 I would request a clarification on scope and depth of the cyber assets that authorize and/or log access to the PSP. The previous language would have limited the devices to those that performed control and monitoring of the PSP (traditional physical access control security systems, and localized panels that communicate with the main system). The new language provided in the draft under CIP-006-2 R2 modifies the scope to include cyber assets that authorize and/or log access to the PSP. I am concerned with the depth of devices involved in the authorization or logging chain. Specifically: log correlation servers, backup and recovery servers, camera's, badge printing workstations, camera monitoring stations, log printers, etc.. In the current draft it is unclear whether the device performing the authorization and/or logging is the only cyber asset that is subject to the requirements specified in CIP-006-2 R2.1-R2.2 or if all devices involved in authorization or logging are subject to those requirements specified in CIP-006-2 R2.1-R2.2. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets that authorize and/or log access to the PSP. Regarding CIP-006-2 R3 I reiterate my request for a clarification on scope and depth of the devices to be included in the access control and/or monitoring of the ESP. The previous language would have limited the devices to those that performed access control and monitoring of the ESP (traditional Firewalls, routers with ACL's, any IPS devices, VPN endpoints, etc.). The new language provided in the draft under CIP-005-2 R1.5 modifies the scope to include cyber assets used in the access control and/or monitoring of the ESP. I am concerned with the depth of devices involved in the monitoring chain that have no relevance on access control, but are an active component in the monitoring of the ESP. Specifically: log correlation servers, SNMP trap servers, SMTP relay servers for notification, pagers, blackberry's, enterprise email servers, backup and recovery servers for these extended devices, etc.. In the current draft it is unclear whether the device performing the monitoring is the only device that is subject to the requirements specified in CIP-005-2 R1.5 or if all devices involved in monitoring are subject to those requirements specified in CIP-005-2 R1.5. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets used in the monitoring of the ESP. When providing the scope and depth clarification of these cyber assets, the drafting team needs to give consideration in regards to an entities ability to satisfy the new CIP-006-2 R3 requirements of containing all of the cyber assets used in the access control and/or monitoring within an identified PSP. In regards to CIP-006-2 R4-R6, I believe the sub requirement identifiers were removed as they are not specific requirements, but rather a means to satisfy the requirement. I believe the bullet items need some level of identifier for reference purpose. Potentially a B4.1, B4.2, etc. this would allow for an entity to

Organization	Yes or No	Question 5 Comment
		reference the manner in which they satisfy the requirement.
Response: **The drafting team agrees that not all of the changes were clearly identified. However, the posted version (the one that was commented on) is the official version, and while the drafting team did renumber some of the requirements, these are consistent across the reliability standards.** **In relation to your comments on CIP-006-2 R2 and R3, the intent of the modification was to clarify that a device that performs either function must be included. However an unintended consequence of this change was to add ambiguity as to what constitutes a monitoring device. The intent is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **With respect to your comments on CIP-006-2 R4-R6, while the drafting team did renumber some of the requirements, these are consistent across reliability standards. The changes from individual sub-requirements to bullets were made to correct an original error where requirements cannot be levied upon an item that may not be implemented.**		
CoreTrace		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	Requirement R2.1 will limit the ability of entities to leverage existing personnel to perform such duties as allocating access cards to legitimate visitors. Such duties are frequently delegated to trained reception personnel. OPG believes that allowance must be made for workstations in reception areas and selected offices areas (e.g. Human Resources departments). Cyber controls such as dual authentication on the workstation would be sufficient to meet the protective needs of the system. As noted earlier with respect to CIP 005-2 R1.5, OPG believes that CIP-006-2 R3 creates issues where an entity may be using a third party to remotely monitor and administer Cyber Assets used in the control

Organization	Yes or No	Question 5 Comment
		or monitoring of the ESP. The new requirement will require the entity to police the physical security measures of any such third party to a degree not required for third parties who may support CCAs within the ESP. OPG suggests that the requirements for Cyber Assets used in the access control and / or monitoring of the ESP require protections to the same standards as those which are used to access CCAs. With respect to R1.6 there is concern that the addition of the new word "continuous" it will be difficult to demonstrate compliance. Requirements need to be enforceable. We recommend removing "continuous". We are concerned with the change in R1.7 reducing the time to update the Physical Security Plan from 90 to 30 calendar days. In a large organization this timeframe may not be achievable. Changes to CIP-006 R1.1 open up concerns about the protection of non- Critical Cyber Asset components such as cables. To eliminate this concern we request that the wording of the last sentence be returned to read "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets."
Response: **Any device that has the ability to authorize and or log access to Physical Security Perimeters must be physically protected per requirement CIP-006-2 R2.** **Relating to your comment on CIP-006-2 R3, the Requirements apply regardless of who performs the functions.** **The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted).** **For consistency across all CIP standards, short term implementations were reduced from 90 days to 30 days.** **Requirement 1.1 specifically addresses Cyber Assets and not a subset of Critical Cyber Assets. Any device that is within the same Electronic Security Perimeter as a Critical Cyber Asset must be within a Physical Security Perimeter, and hence must be addressed within the Physical Security plan**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.

Organization	Yes or No	Question 5 Comment
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	No	With respect to individual bullet points: (i) R1: The reference to the Senior Manager should also refer to CIP-003 R2 to clarify the requirement. (ii) CIP-006 R1.6 should not require "continuous" escorted access, since demonstrating compliance with such requirement would be impossible. As an alternative, wording might indicate that visitors are to be escorted in a manner that ensures their actions can be supervised and unauthorized disclosures prevented, and/or only authorized employees can be escorts. (iii) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" (iv) R1.4, reference to R3 should read R4.
Response: **(i) The drafting team feels we made this distinction by the change from "a Senior Manager" to "the Senior Manager".** **(ii) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted).** **(iii) The drafting team feels the statement is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **(iv) The drafting team agrees and will implement this change.**		

Organization	Yes or No	Question 5 Comment
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	No	Xcel Energy feels strongly that 30 days is too short of a time frame to get drawings updated, Sr. Management approval,..etc. every time there is a change to the plan. We feel that 60 calendar days is more attainable industry-wide.
Response: **The drafting team understands your concerns, however for consistency across all CIP standards, short term implementations were reduced from 90 days to 30 days.**		
ISO New England Inc	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous." it is subjective and will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar daysof the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any"
Response: **1) Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2) The drafting team agrees and will implement this change.** **3) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).** **4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your**		

Organization	Yes or No	Question 5 Comment
comments as appropriate if they have not been addressed.		
American Transmission Company	Yes	
TVA	No	We agree with all except, CIP-006 R1.6. CIP-006 R1.6 requires a "continuous" escort. We agree that performing escort duties in a manner that ensures visitors actions are supervised and malicious attempts are prevented is critical. However, being able to provide auditable proof of "continuous" escorting creates a condition that is impossible to meet. We propose the following: R1.6: Policy and procedures describing roles, responsibilities, and corrective action in regard to escorting personnel not authorized for unescorted access within the Physical Security Perimeter. We would also recommend that Responsible Entitie obtain a signature for record from individuals performing escort duties demonstrating that they acknowledge and accept their role and responsibilities and understand what corrective actions will be taken for any breach in procedure.
Response: **The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted).**		
Duke Energy	No	The language introduced in R2 and R3 has created an inconsistency with the use of the phrases "authorize and/or log access" and " access control and/or monitoring". This creates confusion and opportunity for differing interpretations of the requirements.
Response: **Issues such as inconsistencies will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
Brazos Electric Power Cooperative, Inc.	No	In R1.3, replace "the perimeter(s)" with "the Physical Security Perimeter(s)". In R8.3, need to clarify what "outage records" are. In M2, replace "shall make available documentation that" with "shall make available documentation showing how " In M3, replace "shall make available documentation that" with "shall make available documentation

Organization	Yes or No	Question 5 Comment
		showing how".
Response: **The drafting team feels it is clear that the perimeters are "physical" since the requirement is directed at Physical Security Perimeters. Requirement 1.3 is a sub requirement of R1, "Physical Security Plan".** **With respect to your comments on R8.3, M2, and M3 issues, these will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns have not been addressed.**		
Progress Energy	Yes	CIP006R1.7 – We believe the reduction of 90 to 30 days for updates to the Physical Security Plan is inadequate when you consider the number and levels of approvals required to complete the updates. PE recommends leaving the 90 day time period.
Response: **For consistency across all CIP standards, short term implementations were reduced from 90 days to 30 days.**		
Standards Review Committee of ISO/RTO Council	No	(i) R1: We recommend revising "the Senior manager" to "a senior manager" as the requirement should not be job title specific. Further, the reference to "a Senior Manager" also should be made to CIP-003 R2 to clarify the requirement. (ii) CIP-006 R1.6 should not require "continuous" escorted access, insofar as that would create a condition that is impossible to prove to auditors. As an alternative, wording might indicate that visitors are to be escorted in a manner to ensure their actions can be supervised and unauthorized disclosures prevented, and/or only authorized employees can be escorts. (iii) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" (iv) R1.4, reference to R3 should read R4.
Response: **(i) The drafting team feels it made this distinction by the change from "a Senior Manager" to "the Senior Manager".** **(ii) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted).**		

Organization	Yes or No	Question 5 Comment
(iii) The drafting team feels the statement is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters. **(iv) The drafting team agrees and will implement this change.**		
KEMA	Yes	In R4 and R6, access control and logging should include in and out of the Critical Facility in accordance to NERC's Security Guidelines for the Electricity Sector: Physical Security--Substations Dated 10-2004. Responsible entities should control and log in and out access to Critical Facilities to maintain a high level of access security to Critical Cyber Assets.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Austin Energy	No	The original stated intent of the Standards was to protect against 'cyber' attacks. Modifications to R2 would seem to overstep the intent in the case where a separate non-critical system was used the monitor assess to Critical Cyber Assets (CCA). Now if the CCA was itself incorporated into the physical assess monitoring then the modification to R2 is self evident. However, when a separate system is employed, it takes a coordinated effort by humans with a physical presence to pull off an attack. Although this may certainly qualify as espionage, there is nothing 'cyber' about it. It is proposed that an exception be made for cases where a separate system is used to monitor CCA.
Response: **The original standards were to protect the Cyber Assets from both cyber and physical attacks. While most of the standards deal with cyber protections, the easiest method to successfully attack a cyber asset is through physical means. The modifications in CIP-006 clarify cyber protections afforded to the systems that assist in the physical protection, including access and monitoring.** **The SDT will clarify that monitoring systems that do not authenticate and/or grant physical access are excluded from this requirement. An example would be a CCTV system that performs the monitoring role and also supports access logging, but does not control the Physical Security Perimeter access point.**		
Kansas City Power &	Yes	

Organization	Yes or No	Question 5 Comment
Light		
San Diego Gas and Electric Co.	No	SDG&E has the following comment to make about CIP-006-2 R2.1: This requirements states that cyber assets that authorize and/or log access to PSPs must be "protected from unauthorized physical access." In addition, R2.2 states that these cyber assets must be afforded the protective measures specified in, among others, CIP-006-2 R4, which addresses physical access control. Including both of these statements seems redundant. We recommend removing R2.1 and appending the text of R2.2 to R2 (thus allowing the deletion of R2.2)
Response: **The SDT respectfully disagrees with the comment. The Reference in R2.2 to CIP-006-2, R4, defines the procedural and operational control requirements for the Physical Security Perimeter access points (e.g., doors with card access readers or other access authentication processes). R2.1 refers specifically to protecting the authorization and logging systems, recognizing that in some cases it is not practical to require that the systems reside within a defined Physical Security Perimeter.**		

6. The CSO706 SDT is proposing the following modifications to **CIP 007-1:**

   - Add "implement" to CIP-007-1 Requirements R2, R3 and R7 to clarify that processes and procedures must be implemented as well as documented.
   - Remove the "acceptance of risk" language (per FERC Order 706, paragraph 622) in Requirements R2.3, R3.2 and R4.1.
   - Revise the timeframe for documenting changes to systems or controls to thirty days in Requirement R9.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 6 Comment
Detroit Edison Company	Yes	
PacifiCorp	No	Other comment: R5.3 - Instead of prescribing specific password construction standards, it would be better to express desired outcomes in terms of measurable entropy. The standards should require a certain level of protection against password guessing and brute force "hash cracking" attacks, but leave specifics to the implementers. For example, the standard could simply require 24 bits min-entropy per NIST Special Publication 800-63.
Response: **R5.3 was not changed during this revision of the CIP standards. These types of issues will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	Comment: MidAmerican does not agree with the change within the Purpose section of the standard to change the term ?non-critical? to ?other.? MEC proposes the following language Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical (delete other) cyber assets and cyber assets used in access control and/or monitoring within the Electronic Security Perimeter(s) . Standard CIP- 007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

Organization	Yes or No	Question 6 Comment
Response: **The word "non-critical" will be put back into the purpose statement within parentheses beside the word other [i.e "other (non-critical)"], which is similar to the structure in the implementation plan. The additional wording is meant to remove ambiguity.**		
Northeast Power Coordinating Council	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the entity's change process."
Response: **Each entity's change process may be different and processes may include a number of steps to be performed after the actual change is completed over an extended period of time. The proposed wording would not drive a consistent approach to having documentation completed within thirty days of the actual modification to the systems or controls.**		
WECC Reliability Coordination	No	R2.3, R3.2 and R4.1 removes an organizations ability to accept minimal risk which cannot be compensated for.R9, we think 90 days is a reasonable time frame, 30 days is too restrictive.
Response: **FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. For example, Responsible Entities should implement the requirements for ports and services for all cyber assets within an electronic security perimeter or justify why it is not doing so pursuant to technical feasibility exceptions including reporting requirements and the implementation of compensating measures. The drafting team feels that one entity cannot accept risk for another entity in an interconnected power system. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process (Please refer to FERC Order 706, Paragraph 151).** **(FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Southern Company	Yes	CIP-007 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority.

Organization	Yes or No	Question 6 Comment
		CIP-007 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-007 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. We recommend striking the following language from the Purpose section - "those systems determined to be Critical Cyber Asset, as well as the other". – General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: **1) The word non-critical will be added back into the purpose statement within parentheses beside the word other [i.e "other (non-**		

Organization	Yes or No	Question 6 Comment
		critical)"], which is similar to the structure in the implementation plan. The additional wording is meant to remove any ambiguity. 2) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit. 3) The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence. The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process." See comments to question 5.
Response: Since each entity's change process may be different and since processes may include a number of steps to be performed after the actual change is completed over an extended period of time, the newly proposed wording will not drive consistency in having documentation completed within thirty days of the actual modification to the systems or controls.		

Organization	Yes or No	Question 6 Comment
Southern California Edison Company	No	The change from 90 days to 30 days is difficult to achieve. SCE suggests 60 days to provide ample time for internal due diligence.
Response: **(FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Tampa Electric Company	No	Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	Yes	We fully support the revisions in section B, Requirements.

Organization	Yes or No	Question 6 Comment
Response: **Thank you for your comment.**		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS do not agree with the change within the Purpose section of the standard to change the term “non-critical” to “other.” The term "other" is too vague. The MRO NSRS proposes the following language: Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical (delete other) cyber assets and cyber assets used in access control and/or monitoring within the Electronic Security Perimeter(s) . Standard CIP- 007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
Response: **The word non-critical will be added back into the purpose statement within parentheses beside the word other [i.e “other (non-critical)”], which is similar to the structure in the implementation plan. The additional wording is meant to remove any ambiguity.**		
Pepco Holdings, Inc - Affiliates		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e., a documentation of a formal security management program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	No	Recommendation to increase the timeframe in R9 to document changes to systems or controls to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation.

Organization	Yes or No	Question 6 Comment
Response: **(FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Old Dominion Electric Cooperative		
City of Tallahassee (TAL)	Yes	Although the "acceptance of risk" ties in with the discusson above on business judgement.
Response: **The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	More rational is needed to explain the decision to remove "acceptance of risk" and "reasonable business judgement" language from CIP requirements while leaving the ability to identify "exceptions" through cyber security policy (CIP-003-2, R3.) With this exception in place, entities will be able to establish "policy" that will allow for deviation from the requirements outlined in the Standards. If the intent of the changes was to limit implementation disparity across all entities by removing "risk based decisions", the potential remains that an entity will establish exceptions through relaxed "policy" and the disparity will remain. If the intent was to remove any avenue for not meeting or implementing the requirements, entities may continue to accept "risk based decisions" (although not formally identified as such) by

Organization	Yes or No	Question 6 Comment
		pursuing relaxed policy via exceptions (CIP-003-2 R3).Further, entities may have numerous "systems" of differing capabilities and generations. To require that exceptions be documented in "policy" does not acknowledge the diversity of systems that may be in service in an organization in as effective a manner as documenting exceptions as a function of the system, its environment, and its criticality. Such documentation would be better addressed through specific risk-acceptance decisions tied to specific systems, rather than to an all-encompassing "policy. "Finally, as CIP-003 is amended, entities may not implement or meet certain requirements, as long as, they are identified and documented as "policy exceptions." Was this the intent of the authors? We recommend that risk-managed approaches to cyber security requirements be reinstated into the requirements, recognizing that such a change will require FERC to reassess their order.
Response: **The recommendation of using a risk-managed approach to cyber-security requirements is well appreciated and will be a significant topic in the next revision phase of the CIP Standards.** **The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.**		
Orange and Rockland Utilities Inc.	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process."
Response: **Since each entity's change process may be different and since processes may include a number of steps to be performed after the actual change is completed over an extended period of time, the newly proposed wording will not drive consistency in having documentation completed within thirty days of the actual modification to the systems or controls.**		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator	Yes	
Dynegy	Yes	

Organization	Yes or No	Question 6 Comment
Northern Indiana Public Service Company	No	Within the purpose section of CIP-007-2 I would recommend the removal of the following language "those systems determined to be Critical Cyber Assets, as well as the non critical" as this language is redundant.
Response: **The word non-critical will be added back into the purpose statement within parentheses beside the word other [i.e "other (non-critical)"], which is similar to the structure in the implementation plan. The additional wording is meant to remove any ambiguity.**		
CoreTrace	No	The modifications above are acceptable, however R4.2, as written, implies that all anti-virus and malware prevention tools have signatures, which is not true. Specifically whitelisting or behavioral approaches do not require signature updates. Whitelisting in particular provides greater antivirus/antimalware protection than traditional signature based antivirus, including zero day protection, yet does NOT require "signatures". Whitelisting relies on a positive security model that complements CIP 003 Configuration Control Requirements. By clarifying that traditional signature based antivirus is not required, NERC opens up the range of platforms and systems that can be protected greatly. For example, traditional antivirus does not exist for most Unix based systems, however whitelisting does. Propose revising R4.2 to read as follows: R4.2. If the Responsible Entity chooses to implement signature based antivirus or malware prevention tools the Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention ?signatures.? The process must address testing and installing the signatures. This requirement does not apply for non-signature based antivirus or malware prevention tools such as those based on whitelisting or behavioral analysis.
Response: **R4.2 was not changed during this revision of the CIP Standards. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	Reducing the timeframe for documenting changes to systems or controls in R9 from 90 to 30 calendar days introduces a constraint that may not be achievable in a large organization.

Organization	Yes or No	Question 6 Comment
Response: **(FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	No	Acceptance of risk for certain ports and services is within security best practices. Mitigating controls for certain ports and services could effect the reliable operation of the bulk electric system.
Response: **FERC directed the ERO to have a technical feasibility exception process supersede all instances of acceptance of risk. For example, Responsible Entities should implement the requirements for ports and services for all cyber assets within an electronic security perimeter or justify why it is not doing so pursuant to technical feasibility exceptions including reporting requirements and the implementation of compensating measures. The drafting team feels that one entity cannot accept risk for another entity in an interconnected power system. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process (Please refer to FERC Order 706,**		

Organization	Yes or No	Question 6 Comment
Paragraph 151).		
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process."
Response: **Since each entity's change process may be different and since processes may include a number of steps to be performed after the actual change is completed over an extended period of time, the newly proposed wording will not drive consistency in having documentation completed within thirty days of the actual modification to the systems or controls.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	Regarding R2.3, R3.2 and R4.1, we understand that the Responsible Entity's action to document compensating measures is sufficient to achieve compliance with the requirements, and that the Responsible Entity does not need to also invoke the "Technical Feasibility" exception. Technical Feasibility is only applicable when the Responsible Entity cannot comply with a requirement. We also recommend that the Responsible Entity be required to perform an analysis of the residual risk after all compensating measures are applied. Add the words "and analysis of residual risk" to the end of R2.3, R3.2 and R4.1
Response: **FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process. [Please refer to FERC 706, Paragraph 151]** **The Technical Feasibility Exception process is under development by NERC staff. Please readdress this issue during the Phase 2 comment period.**		

Organization	Yes or No	Question 6 Comment
Brazos Electric Power Cooperative, Inc.	No	1) In R5.1.1, replace "user accounts" with "user access privalges". 2) In R6.4, replace "all logs" with "all logs of system events related to cyber security". 3) In M2, replace "available documentation" with "available documentation of all ports and services".
Response: **1) All aspects of R5.1 are specific to individual and shared system accounts. User access privileges are covered in CIP-004.** **2) The requirement is to retain all logs from all applicable cyber assets for 90 days. Log retention of system events related to cyber security may be longer based on incident response and reporting plan as defined by CIP-008.** **3) The SDT reviewed and concluded that changing the wording as suggested would exclude the process documentation. It remains applicable to all documentation related to R2.**		
Progress Energy	Yes	CIP007R9 – The reduction from 90 to 30 days is inadequate. PE recommends leaving the 90 day time period (same justification as for CIP006-R1.7).
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

7. The CSO706 SDT modified **CIP-008-1** Requirement R1 to clarify the requirement to implement the plan in response to cyber security incidents, update the plan within thirty days of any changes, and clarify that tests of the plan do not require removing components or systems during the test.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 7 Comment
Detroit Edison Company	No	The addition of "and implement the plan in response to Cyber Security Incidents." is awkward. This literally states that the plan will only be implemented upon a security incident, but the plan must be implemented in order to "characterize and classify" reportable Cyber Security Incidents. It might be clearer if written as " The Responsible Entity shall develop, implement and maintain a Cyber Security Incident Response Plan....and execute the plan in the event of a Cyber Security Incident." Remove the "Process for?." language in CIP-008-2 R1.4, R1.5, and R1.6 to be consistent with the language changes in CIP-006 R1.7 and R1.8. Suggested language is as follows: R1.4. Update of the Cyber Security Incident response plan within thirty calendar days of any changes.R1.5. Annual review of the Cyber Security Incident response plan.R1.6. Annual testing of the Cyber Security Incident response plan. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
PacifiCorp	Yes	
FirstEnergy Corp	Yes	
MidAmerican Energy Company	Yes	

Organization	Yes or No	Question 7 Comment
Northeast Power Coordinating Council	No	1) - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2) - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within thirty calendar days of completion of the entity's change process". 3) - Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
Response: **1)-2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **3) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
WECC Reliability Coordination	No	we feel that 90 days is a reasonable time frame.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Southern Company	Yes	CIP-008 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-008 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-008 Section D - Compliance: 1.4.2 - Should have a time limit to reduce the overall liability of

Organization	Yes or No	Question 7 Comment
		confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.2 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. We are confused about the necessity to call out a specific "Cyber Security Incident" response team. Does this no longer require an entity to have a physical security incident response team? -- General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Organization	Yes or No	Question 7 Comment
Response: **1. This standard relates to cyber security incident response only. An entity's physical security incident response may or may not be related.** **2) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **3. The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence.** **The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.** **The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1) - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2) - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response

Organization	Yes or No	Question 7 Comment
		plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within thirty calendar days of completion of the Entity's Change Process" (see questions 5). 3) - The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4) - Measure M1 is one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
Response: **1)-3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
Southern California Edison Company	Yes	
Tampa Electric Company	No	Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms

Organization	Yes or No	Question 7 Comment
		or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	No	The sentence added to the end of R1.6 would be more appropriate in a FAQ, guideline, or interpretation rather than in the standard itself.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS questions the change in timing requirements for R1.4 from 90 days to 30 days. What is the justification for change? Do you have specific examples of problems that resulted from the plan not being updated within 90 days.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Pepco Holdings, Inc - Affiliates		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal incident management program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).

Organization	Yes or No	Question 7 Comment
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	No	Recommendation to increase the timeframe in R1.4 to document changes to the cyber security incident response plan to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Old Dominion Electric Cooperative		
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	Yes	
Orange and Rockland Utilities Inc.	No	1) We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain, and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2) We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within within thirty calendar days of completion of the Entity's Change Process"

Organization	Yes or No	Question 7 Comment
		3) The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4) Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
Response: **1)-3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
CenterPoint Energy	No	CenterPoint Energy strongly disagrees with the proposed modification in R1.4 reducing the amount of time allowed for making changes and updates to the Cyber Security Incident Response Plan from 90 days to 30 days. Furthermore, the Commission did not direct this change in Order 706 or Order 706A. CenterPoint Energy believes 30 days is too constraining and unwarranted, and that 90 days should be retained. If the SDT moves forward with the proposed reduction in time, CenterPoint Energy proposes 60 days to allow for a complete review of any changes.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Manitoba Hydro	Yes	
Alberta Electric System Operator	Yes	
Dynegy	Yes	
Northern Indiana Public	No	In CIP-008-2 R1.2, I would like a clarification of the additional language detailing Cyber Security Incident

Organization	Yes or No	Question 7 Comment
Service Company		response team requirements. This additional language implies Cyber Security specific training or a core set of knowledge requirements for the incident responders. What will be the measuring stick to determine if an incident responder is a Cyber Security Incident responder or a non-cyber security incident responder?
Response: **Team members should be able to effectively perform the roles and responsibilities outlined in the Cyber Security Incident Response Plan.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	Reducing the timeframe to update the Incident Response Plan from 90 to 30 calendar days introduces a constraint that may not be achievable in a large organization.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was**		

Organization	Yes or No	Question 7 Comment
written to support this concept. **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	No	The new sentence in R1.6 is not a requirement and does not add any value; in fact, it may create confusion - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1) - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop. and maintain a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident, when such an incident occurs." 2) - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within within thirty calendar days of completion of the Entity's Change Process" 3) - The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4) - Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a

Organization	Yes or No	Question 7 Comment
		requirement incorrectly.
Response: **1)-3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	No	In R1.3, replace "Process for reporting" with "Process for communicating reportable". In R1.4, replace "of any changes" with "of any procedural changes". In M2, replace "all documentation" with "all relevant documentation related to Cyber Security Incidents".
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Progress Energy	Yes	CIP008R1.4 – The reduction from 90 to 30 days is inadequate considering the coordination and approvals necessary. PE recommends leaving the 90 day time period (same justification as for CIP006-R1.7).
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		

Organization	Yes or No	Question 7 Comment
Standards Review Committee of ISO/RTO Council	No	The new sentence in R1.6 is not a requirement and does not add any value; in fact, it may create confusion - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

8. The CSO706 SDT revised the timeframe to thirty days for communicating updates of recovery plans to personnel responsible for activating or implementing the plan in **CIP-009-1** Requirement R3.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 8 Comment
Detroit Edison Company	Yes	
PacifiCorp	Yes	
FirstEnergy Corp	Yes	
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	No	1) We recommend changing R3 from "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed." to "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of completion of the entity's change process." 2) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate.

Response:

1) The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.

2) **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**

Organization	Yes or No	Question 8 Comment
WECC Relibaility Coordination	No	We feel 90 days is a reasonable time frame.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Southern Company	Yes	
Luminant Power	Yes	
Encari	No	General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 1) The wording of 1.1.1 is awkward and should be modified. 2) We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: **1) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **2) The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.** **The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity**		

Organization	Yes or No	Question 8 Comment
has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1) We recommend changing R3 from "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of the change being completed." to "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of completion of the Entity's change process." 2) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate
Response: **1) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
Southern California Edison Company	Yes	
Tampa Electric Company	No	Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."

Organization	Yes or No	Question 8 Comment
Response: **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	No	The MRO NSRS questions the change in timing requirements for R3 from 90 days to 30 days. What is the justification for change? Do you have specific examples of problems that resulted from the plan(s) not being updated within 90 days.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Pepco Holdings, Inc - Affiliates	No	It may not be possible to communicate updates of recovery plans to all personnel responsible for activating or implementing the plan within 30 days (e.g. family leave). Suggest adding exceptions.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this**		

Organization	Yes or No	Question 8 Comment
project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	No	Recommendation to increase the timeframe in R3 to require updates to be communicated within 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management activity.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	Yes	
Orange and Rockland Utilities Inc.	No	1) We recommend changing R3 from "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of the change being completed." to "Updates shall becommunicated to personnel responsible for the activation and

Organization	Yes or No	Question 8 Comment
		implementation of the recoveryplan(s) within thirty calendar days of completion of the Entity's change process." 2) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate
Response: **1) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards..**		
CenterPoint Energy	No	Regarding R3, CenterPoint Energy acknowledges that updates to a recovery plan and communication of those updates should be completed in a timely manner; however, CenterPoint Energy believes the SDT went too far in reducing the timeframe for communicating updates from 90 days to 30 days. CenterPoint Energy believes that 30 days is too constraining. Furthermore, in FERC Order 706, paragraph 731, the Commission separated the time allowed for updating recovery plans (30 days) and the time allowed for communicating those updates (90 days), and was willing to consider timeframes other than 30 days. CenterPoint Energy proposes a 60 day window for updating a recovery plan and retaining the 90 day window for communicating the updates to responsible personnel. This would allow adequate time for the appropriate documentation changes to be made and is still timely for communicating to personnel.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Manitoba Hydro	Yes	
Alberta Electric System Operator	Yes	
Dynegy	Yes	

Organization	Yes or No	Question 8 Comment
Northern Indiana Public Service Company	No	I do not agree with the reduction from 90 to 30 days. I would propose to provide uniformity and match the modified requirement under CIP-007-2 R9, which requires the modifications to be documented within 30 calendar days after completion versus the CIP-009-2 R3 language which requires the updates to be communicated within 30 calendar days after completion.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	Reducing the timeframe to communicate updates to CCA recovery plans from within 90 to within 30 calendar days introduces a constraint that may not be achievable in a large organization.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was**		

Organization	Yes or No	Question 8 Comment
written to support this concept. **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1 - We recommend changing R3 from "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of the change being completed." to "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of completion of the Entity's change process." 2 - "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate.
Response: **1) The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2) The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		

Organization	Yes or No	Question 8 Comment
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	No	In R3, replace "being completed" with "being effective".
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Progress Energy	Yes	CIP009-R3 – The reduction from 90 to 30 days is inadequate considering the coordination and approvals necessary. PE recommends leaving the 90 day time period (same justification as for CIP006-R1.7).
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	In R1, it should be added that the Recovery Plans must be stored on site and a second copy off-site for responders in case the primary site is inaccessible.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific**		

Organization	Yes or No	Question 8 Comment
directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

9. The CSO706 SDT proposes the following for the **Effective Date**:

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

   Do you agree with the proposed Effective Date? If not, please explain and provide an alternative to the proposed effective date that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 9 Comment
Detroit Edison Company	No	Does this mean that the current quarter must end, and then you start counting to the first day of the following 3 quarters, or do you include the current quarter in counting? Why not simplify things and use a number of days, such as: "120 calendar days after applicable regulatory approvals have been received . . . . . ."
Response: **The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.**		
PacifiCorp	No	This effective date as written could move the compliance date for our GO functions up 6 months from the previously published compliance schedule found in Table 3. PacifiCorp has been working toward compliance with the standards under the premise that the generation owner has until December 31, 2009, to become compliant with Version 1 standards. For significant changes proposed in Version 2, the generation owner will need time to address and comply.
Response: **The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions.**		

Organization	Yes or No	Question 9 Comment
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	Comment: This effective date as written could move the compliance date for our GO functions up 6 months from the previously published compliance schedule. MidAmerican Energy Company has been working toward compliance with the standards under the premise that the generation owner has till December 31, 2009, to become compliant with version 1 standards. For significant changes proposed in version 2, the generation owner will need time to address and comply. For applicable regulatory approvals received between January 1 and March 31, revised standards will be effective the following January 1.MEC proposes the following language: Effective Date: The first day of the calendar quarter after at least nine months following the applicable regulatory approvals have been received, as illustrated in the following table. Applicable regulatory approval received - Effective the following Jan. 1- Mar. 31 Jan. 1Apr. 1- June 30 Apr.1July 1- Sept. 30 July 1Oct. 1- Dec. 31 Oct. 1
Response: **The drafting team anticipates that the Phase I revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions. The drafting team believes the six to nine month implementation plan is reasonable.**		
Northeast Power Coordinating Council	No	1) - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)". In addition, Canadian members of NPCC have concerns regarding the standards becoming effective at different dates in different jurisdictions. Coordination is required among government authorities to ensure that standards become effective at the same time in all jurisdictions. 2) - Request confirmation that these Effective Dates apply to these updates (Version 2). 3) - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4) - We request clarification on Compliance 1.1.1. Wording is confusing. 5) - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary, the

Organization	Yes or No	Question 9 Comment
		new terms are not (Regional Entity and Compliance Enforcement Authority). 6) - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7) - Clarification required for "the last audit records" and "subsequent audit records" in Data Retention 1.4.2. This comment applies to CIP-002 - CIP-009.

Response:

1) The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.

For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2. The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved.

3. The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.

4. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.

5. The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.

Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and

Organization	Yes or No	Question 9 Comment
ByLaws. **6. The Violation Severity Levels (VSLs) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team.** 7. **The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	
Luminant Power	Yes	
Encari	No	This effective date is still open-ended as the process is not complete. Once additional comment periods have completed and the revisions have been refined we will provide comment as to the acceptability of this timeframe and the continued assurances of the reliability of the Bulk Electric System. We recommend that the standards become agreed upon and complete and then an effective implementation date be identified. This will provide proper assurances from asset owners that they can indeed meet the timeframe identified while continuing to assure the reliability of the BES. We also are confused regarding the term "calendar quarter" versus a concept of "fiscal quarter". Please provide a clarification.
Response: **The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.**		
TransAlta Centralia Generation, LLC	Yes	

Organization	Yes or No	Question 9 Comment
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1. Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2. Request confirmation that these Effectives Dates apply to these updates (Version 2) 3. We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4. We request clarification on Compliance 1.1.1. Wording is confusing. 5. While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6. When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7. There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009

Response:

1. The proposed language does not differ significantly from the original language, so the benefit of the proposed modification is not clear. The suggested language was not adopted. The language in the "proposed effective date" section of the standard is the same language that has been used in proposed standards for the past several months, and most entities have indicated acceptance of this language.

For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2. The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the

Organization	Yes or No	Question 9 Comment
previous version that was already approved. **3. The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.** **4. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.** **5. The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.** **Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **6. The Violation Severity Levels (VSLs) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team.** 7. **The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.**		
Southern California Edison Company	No	Wording is ambiguous. SCE suggests "six (6) months from date of approval."
Response: **The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.**		
Tampa Electric Company	Yes	

Organization	Yes or No	Question 9 Comment
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates	Yes	Please consider adding in parenthesis "approximately 270 days" after "the third calendar quarter" for clarification. "The first day of the third calendar quarter (approximately 270 days) after applicable approvals?"
Response: **The NERC Compliance program has requested the implementation date start on a calendar quarter January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	

Organization	Yes or No	Question 9 Comment
City of Tallahassee (TAL)	Yes	It is confusing though.
Response: **Thank you for your comment.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	Yes	
Orange and Rockland Utilities Inc.	No	1 - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2 - Request confirmation that these Effectives Dates apply to these updates (Version 2) 3 - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4 - We request clarification on Compliance 1.1.1. Wording is confusing. 5 - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6 - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7 - There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009

Organization	Yes or No	Question 9 Comment

Response:

1. **The proposed language does not differ significantly from the original language, so the benefit of the proposed modification is not clear. The suggested language was not adopted. The language in the "proposed effective date" section of the standard is the same language that has been used in proposed standards for the past several months, and most entities have indicated acceptance of this language.**

   For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2. **The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved.**

3. **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.**

4. **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.**

5. **The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.**

   Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.

6. **The Violation Severity Levels (VSLs) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team.**

7. **The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated**

Organization	Yes or No	Question 9 Comment
documentation.		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator		
Dynegy	Yes	
Northern Indiana Public Service Company	No	I have difficulty responding with acceptance or denial of an implementation schedule when I am not fully aware of what the final draft is going to consist of. Secondly, as this language stands I would like to see a proposed time line based on an example NERC BOT adoption date. I am unclear on weather the Version 2 standards would be implemented in parallel with the existing version 1 implementation schedule, in series, or only begin implementation after FERC approval as this draft is occurring due to FERC directed changes. I am also slightly confused on the audit process and which version of various CIP requirements would be applicable as the responsible entities move into an AC status, while the Version 2 standards could be BOT approved but not FERC approved.
Response: **The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.** **The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions.** **The New Critical Cyber Asset Implementation Plan incorporates Table 4 of the Version 1 Implementation Plan and supersedes the**		

Organization	Yes or No	Question 9 Comment
Version 1 Implementation Plan. The New Critical Cyber Asset Implementation Plan states that "the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the [compliant] milestone listed in this Implementation Plan."		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation		
American Electric Power	Yes	To add further clarity, AEP suggests that the following text be added to the effective date statement above." . . . after applicable FERC approvals have been received and such approval is posted in the public registry (or the . . . "
Response: **The SDT does not feel that a change to the standard language is necessary. The US Federal Rulemaking Process requires that the effective date of the approval rule is contained in the text of the Final Rule that is published in the Federal Register.**		
Ontario IESO	Yes	
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1 - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions

Organization	Yes or No	Question 9 Comment
		where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2 - Request confirmation that these Effectives Dates apply to these updates (Version 2) 3 - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4 - We request clarification on Compliance 1.1.1. Wording is confusing. 5 - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6 - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7 - There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009.

Response:

1. **The proposed language does not differ significantly from the original language, so the benefit of the proposed modification is not clear. The suggested language was not adopted. The language in the "proposed effective date" section of the standard is the same language that has been used in proposed standards for the past several months, and most entities have indicated acceptance of this language.**

   For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2. **The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved.**

3. **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2**

Organization	Yes or No	Question 9 Comment
		standards. **4. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.** **5. The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.** **Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **6. The Violation Severity Levels (VSLs) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team.** 7. **The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.**
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
Progress Energy	No	PE would like clarification on the effective date Section A.5. of each standard. Given the nature of some of the requirements to possibly include significant capital investment, we want to ensure there is adequate time given for budget cycle and outage planning. Also, the guidance for identification of CAs is still incomplete which could impact implementation timeframes. PE recommends allowing 12 months after the BOT approval for the effective date.

Organization	Yes or No	Question 9 Comment
Response: **The NERC Compliance program has requested the implementation date start on a calendar quarter (January, April, July, October). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year. The drafting team believes the six to nine month implementation plan is reasonable. The New Critical Cyber Asset Implementation Plan is applicable to newly identified CAs and supersedes the Version 2 implementation schedule.**		
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

10. The CSO706 SDT is proposing a separate **CIP implementation plan** to address newly identified Critical Cyber Assets. In this plan, three specific classes of categories for newly identified Critical Cyber Assets are described. The plan provides an implementation schedule with "Compliant" milestones for each requirement in each category. All timelines are specified as an offset from the date when the Critical Cyber Asset has been newly identified.

    Do you agree with the approach proposed by the SDT for handling newly identified Critical Cyber Assets? If not, please explain and provide an alternative to the proposed milestones that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 10 Comment
Detroit Edison Company	Yes	
PacifiCorp	Yes	
FirstEnergy Corp	No	While we do agree with the overall objective the team is trying to achieve, we do not agree as presently written and offer the following comments: a) The description of Category 1 seems to imply that a Responsible Entity who has a CIP CA and CCA methodology, but did not identify any CCA assets may be given additional time to comply with the CIP standards when they have identified any CCAs on subsequent annual reviews. However, what is not clear is what triggered the new CCA being identified? The Category 1 description should be clear that it does not apply simply based on "error and ommission" if the Responsible Entity's methodologies for CA and CCA identification have not changed and the Responsible Entity simply overlooked an asset that should have been previously identified and protected. If these newly identified assets were in service during their initial CIP asset determination, then the entity was not compliant with their initial asset identification and it should be expected that the entity would file a Self Report and Mitigation Plan to obtain compliance. b) FE believes our above comment on Category 1 also applies to the Category 2 description as it indicates in the second paragraph that it refers to newly identified CCA assets but they are not associated with an addition or modification through construction, upgrade or replacement. Again, if the methodologies have not changed, if there was no merger or acquisition, then what triggered the newly identified existing asset? It should be clear that "error and ommission" do not apply. c) We agree with the provisions described for newly acquired assets through mergers and acquisitions when companies may have had differing methodologies.

Organization	Yes or No	Question 10 Comment
		d) We agree with item 3 regarding "Compliant upon Commissioning" for newly planned upgrades that result in new CA and CCA items. e) In general we found the information to be overly wordy and confusing to understand. We suggest the team attempt to greatly consolidate the information. f) Tables 2 should be adjusted such that it can be read and viewed stand alone to the extent possible from the remaining supporting text. For example, Table 2 has no indication that the numbers refer to "months".
Response: **a) The Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation.** **b) The Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation.** **c) Thank you for your comment.** **d) Thank you for your comment.** **e) The posted version is simplified from early drafts and must address the complexity of the problem.** **f) The tables will be updated to reflect the time period as being in months.**		
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	No	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that the CIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some refer to Version 2 (Table 2), and the Requirements do not match CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon Commissioning) Critical

Organization	Yes or No	Question 10 Comment
		Cyber Assets. 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence. 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Asset in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial communications and the new Asset uses IP communications. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.

Response:

1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that Entity 12 months to comply.

2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All references to Version 1 of the standards within the document will be similarly modified.

3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.

4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date.

5) The SDT agrees that the CCAs should remain in service to avoid a "detrimental effect on the grid." The inclusion of this sentence reinforces that belief. The SDT is concerned that if the sentence is removed, entities may remove the assets from service in order to not be found in non-compliance of the standard, resulting in a "detrimental effect on the grid." Similarly, changing the sentence to require that the assets must remain in service would not allow a brief maintenance outage to allow entities to implement changes associated with bringing the assets into compliance.

Organization	Yes or No	Question 10 Comment
6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. **7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **8) The SDT agrees with the recommendation.** **9) The SDT agrees with the comment and will change the title of the document accordingly.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	
Luminant Power	Yes	
Encari	No	Due to the massiveness of the CCA process, we recommend that this approach needs to be partitioned in to its own comment period.
Response: **The drafting team does not anticipate additional comment periods for the Phase I revisions to the CIP standards.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some reference Version 2

Organization	Yes or No	Question 10 Comment
		(Table 2) and the Requirements do not match the CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.

Response:

1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that Entity 12 months to comply.

2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All references to Version 1 of the standards within the document will be similarly modified.

3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.

4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date.

5) The SDT agrees that the CCAs must remain in service to avoid a "detrimental effect on the grid." The inclusion of this

Organization	Yes or No	Question 10 Comment
sentence reinforces that belief. **6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **8) The SDT agrees with the recommendation.** **9) The SDT agrees with the comment and will change the title of the document accordingly.**		
Southern California Edison Company	Yes	
Tampa Electric Company	Yes	
Electric Market Policy	Yes	1) "Responsible Entity" is not defined in the implementation plan. 2) On page 1 under Implementation Schedule, Item #3 should read: "A new or existing "Cyber" Asset becomes?" 3) On page 2, the first sentence should reference "other" Cyber Assets rather than "non-critical" Cyber Assets to be consistent with the red-line change to CIP-007-2 Purpose. 4) On page 4, bullet "b" perimeter needs to be capitalized.
Response: **1) Responsible Entity is defined in the language of each standard.** **2) The SDT agrees with the recommendation.** **3) The SDT agrees with the recommendation.** **4) The SDT agrees with the recommendation.**		
PPL Corporation	Yes	PPL agrees with different categories of newly identified Critical Cyber Assets and the different

Organization	Yes or No	Question 10 Comment
		implementation schedule for these classes of categories.
Response: **Thank you for your comment.**		
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates	Yes	We specifically appreciate and support the CSO706 SDT efforts in closing the current gap in the CIP standards for compliance of newly identified Critical Cyber Assets by creating three categories with a related implementation schedule.
Response: **Thank you for your comment.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	Will the drafting team include situations that occur through merger and acquisition(M&A)?
Response: **Merger and Acquisition is addressed in the New Cyber Asset Implementation Plan.**		
Exelon	Yes	The 6 month implementation milestones listed for CIP-004-2 Category 2 should instead reflect 6 months from when the new security boundaries and systems get implemented instead of 6 months from the identification of the newly identified Critical Cyber Asset. Entities will not be able to know all the affected personnel until the new physical and electronic security perimeters are defined and implemented.
Response: **The SDT agrees with the comment and will modify the timeframe to 18 months after the new CCA is identified for Category 2 for CIP-004 Requirements R2, R3 and R4.**		
Old Dominion Electric Cooperative	Yes	

Organization	Yes or No	Question 10 Comment
City of Tallahassee (TAL)	Yes	Although it can be confusing also.
Response: **The posted version is simplified from early drafts and must address the complexity of the problem.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	Yes	
Orange and Rockland Utilities Inc.	No	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan is applies to Version 2 because some references Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Assets in an emergency must be

Organization	Yes or No	Question 10 Comment
		replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.
Response: **1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that Entity 12 months to comply.** **2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All references to Version 1 of the standards within the document will be similarly modified.** **3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.** **4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date.** **5) The SDT agrees that the CCAs must remain in service to avoid a "detrimental effect on the grid." The inclusion of this sentence reinforces that belief.** **6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **8) The SDT agrees with the recommendation.** **9) The SDT agrees with the comment and will change the title of the document accordingly.**		
CenterPoint Energy		
Manitoba Hydro	No	The new implementation plan needs to clearly state that the categorization is only applied to newly

Organization	Yes or No	Question 10 Comment
		identified Critical Cyber Assets, and not to all Critical Cyber Assets. The new implementation plan should also state that the categorization of a Critical Cyber Asset expires and is no longer required when that Critical Cyber Asset becomes compliant. Table 2 needs to indicate that the milestones listed are in months. The title for Table 3 needs to be revised to indicate that the table is to be used for Registered Entities which have identified their first Critical Cyber Asset (Category 1), and for newly Registered Entities.
Response: **The New Critical Cyber Asset Implementation Plan repeatedly refers to "newly identified" Critical Cyber Assets. "Compliant Upon Commissioning" also includes Cyber Assets replacing existing Critical Cyber Assets. The categorization is only used to determine the applicable compliance schedule and has no meaning once the Critical Cyber Asset is compliant. The tables will be updated to reflect the time period as being in months.** **Table 2 is applicable to all Registered Entities that have now identified their first Critical Cyber Asset (Category 1) after registration.** **Table 3 is only applicable to newly Registered Entities whether or not they have identified a Critical Asset.**		
Alberta Electric System Operator		
Dynegy	No	Under the Category 2 heading, the proposed method for handling the case of a business merger or acquisition when any of the Responsible Entities involved had previously identified Critical Cyber Assets is inequitable and inconsistent with the proposed handling of the case when all Registered Entities have identified Critical Cyber Assets. Under the Category 2 heading, in the case of a business merger or acquisition when any of the Responsible Entities involved had previously identified Critical Cyber Assets, it really only matters if the acquiring or controlling Responsible Entity had previously identified Critical Cyber Assets. If the acquiring or controlling entity had not previously identified any Critical Cyber Assets it will have no CIP Compliance Program and it should be required to meet the same Category 1 (instead of Category 2) milestones established for the case where neither Registered Entity involved in merger had previously identified any critical Cyber Assets. In addition, in the case when all Registered Entities involved in a merger have identified Critical Cyber Assets the merged Responsible Entity is required to meet Category 2 milestones after one calendar year from the merger date. This provision in effect grants the Merged Responsibility Entity in this case the approximate equivalent of having to meet Category 1 milestones. This approach further justifies the revised approach suggested above for the former case.

Organization	Yes or No	Question 10 Comment
Response: **In the event of a merger or acquisition of a company resulting in a single registered entity, when both entities have existing programs, the Implementation Plan allows one year for the programs to be harmonized. When only one of the entities has an existing program, that program is expected to continue after the merger. In the case of acquisitions of assets resulting in a change in registered entity, if the acquiring company has a program and the acquired asset is already identified as critical, there is one year to harmonize the programs. If the acquiring company does not have a program and the acquired asset is already identified as critical, continuation of the program at the acquired asset is expected to be provided for in the acquisition process, assuming the asset continues to be critical.**		
Northern Indiana Public Service Company	No	Moving through the existing phases, I do not believe the steps provide for a situation in which a utility wishes to improve or strengthen the risk-based methodology. If a utility has an existing CCA and strengthens the methodology process which in turn produces a new CA and in turn new CCA's, the utility would find itself in immediate non-compliance. Based on this situation and using the flow chart contained within the proposed implementation schedule document, the responsible entity would already have an existing CCA, the Cyber assets of the new resulting CA would already be in service, and it would be a planned change as the utility chose to strengthen the existing methodology. The flow chart result would be compliant upon commissioning, and the cyber asset is already in service, therefore the real world result is immediate non-compliance. I believe this is counter productive as NERC and FERC would encourage an entity to strengthen the risk-based methodology. The current proposed implementation schedule would encourage a utility to not strengthen the risk-based methodology over time in order to remain in compliance. I believe additional provisions need to be made.
Response: **The described scenario is defined in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail.**		
CoreTrace		
Oncor Electric Delivery LLC	No	The timeframes in Table 2 are reasonable. However, CIP-002-1 currently specifies that an asset is not designated as a Critical Asset until the annual application of the Risk-Based Methodology. A cyber asset is not a Critical Cyber Asset unless it is essential to the operation of the Critical Asset. Category 3 "Compliant upon Commissioning" is not a current requirement of CIP-002-1 and represents a significant change to the current standard. This seems to imply that the Risk-Based Methodology must be applied continuously, not just annually. "Compliant upon Commissioning" should only apply to replacing existing Critical Cyber Assets. New Critical Cyber Assets identified by CIP-002-1 Requirement R3 should utilize the timeframes in Category 2

Organization	Yes or No	Question 10 Comment
Response: **CIP-002-2, Requirements R2 (Critical Asset identification) and R3 (Critical Cyber Asset identification) state "the Responsible Entity shall review this list at least annually, and update it as necessary." These requirements expect the entity to assess the new asset or Cyber Asset as part of the planning process.**		
Illinois Municipal Electric Agency		
Ontario Power Generation	No	We note that the implementation plan for newly identified Critical Cyber Assets specifies that it applies to "CIP-002-1 through CIP-009-1 and their successor standards". We further notice that in Milestone Category 2 an number of requirements have a six (6) month timeframe specified for compliance. In effect, the identification of a new CCA at an Entity today would be required to be fully compliant with respect to that new newly identified CCA before December 31, 2009 - the Compliant deadline for all other CCAs.
Response: **The drafting team anticipates that the Phase I revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions.**		
American Electric Power	Yes	
Ontario IESO	Yes	We believe the proposed implementation plan is reasonable and appropriate.
Response: **Thank you for your comment.**		
Ameren	Yes	Would like to see a clarification on what is intended by phrase "planned change".
Response: **A "planned change" is any anticipated and planned for change to an asset or Cyber Asset.**		
Consumers Energy	Yes	

Organization	Yes or No	Question 10 Comment
Company		
Xcel Energy	Yes	
ISO New England Inc	No	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some references Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.

Response:

1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that Entity 12 months to comply.

Organization	Yes or No	Question 10 Comment
2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All references to Version 1 of the standards within the document will be similarly modified. **3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.** **4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date.** **5) The SDT agrees that the CCAs must remain in service to avoid a "detrimental effect on the grid." The inclusion of this sentence reinforces that belief.** **6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **8) The SDT agrees with the recommendation.** **9) The SDT agrees with the comment and will change the title of the document accordingly.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.		
Progress Energy	Yes	
Standards Review Committee of ISO/RTO Council	Yes	We believe the proposed implementation plan is reasonable and appropriate.

Organization	Yes or No	Question 10 Comment
Response: **Thank you for your comment.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

11. Do you agree with the **compliance milestones** included in the proposed implementation plan for handling newly identified Critical Cyber Assets? If not, please explain and provide an alternative to the proposed milestones that would eliminate or minimize your disagreement..

Summary Consideration:

Organization	Yes or No	Question 11 Comment
Detroit Edison Company	No	Table 2 does not address CIP-006-2 R7 and R8. They should both be 24 for category 1 and 12 for category 2. Table 2 CIP-008-2 R2 category 2 should be changed from 0 to 6 which matches the timetable associated with R1. The 0 implies that a Responsible Entity needs to retain documents relating to requirement, R1.1, which that entity is not yet required to be compliant. Table 2 CIP-009-2 R2 and R3 category 2 should be changed from 0 to 12. Similarly to the comment around CIP-008-2 R2, a Responsible Entity cannot be compliant with exercising a plan that is not required to exist. Changing the timetable to 12 ensures the recovery plan is initially executed in the annual time frame required by R2.
Response: **Table 2 does not reflect the addition of two new requirements in CIP-006-2. The SDT will update the tables appropriately.** **The formal title and references to the CIP standards will be modified to refer to the Version 2 standards and their successors.** **The SDT will update Table 2 CIP-008-2 R2 category 2 to 6 months as recommended.** **The SDT will update Table 2 CIP-009-2 R2 and R3 category 2 to 12 months as recommended.**		
PacifiCorp	Yes	
FirstEnergy Corp	Yes	We agree with the Implementation Plan times described for Category 1 and Category 2, however, we believe clarification is need as to when these provisions apply. See our comments in Question 10.

Organization	Yes or No	Question 11 Comment
Response: **The Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation.**		
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	No	1 - We recommend that Table 2 clarify the units as months, per page 1. 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 – Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Response: **1) The tables will be updated to reflect the time period as being in months.** **2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	
Luminant Power	Yes	
Encari	No	Due to the massiveness of the CCA process, we recommend that this approach needs to be partitioned in to its own comment period. For instance, the current document details "existing" within CIP-003-2; however - newly identified CCAs may not immediately be able to compliant at zero day with CIP-003-2 requirements. For example R4 requires the information associated with the CCA to be protected. This information may still reside in a non-protected format prior to becoming a CCA - however the

Organization	Yes or No	Question 11 Comment
		implementation timeframe is "existing".
Response: **The drafting team does not anticipate additional comment periods for the Phase I revisions to the CIP standards.** **The SDT agrees with the example cited and will modify the Category 2 compliance time frame for CIP-003-2 Requirements R4, R5, and R6 to be 6 months.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1 - We recommend that Table 2 clarifies the units as months, per page 12 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6.3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Response: **1) The tables will be updated to reflect the time period as being in months.** **2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
Southern California Edison Company	Yes	
Tampa Electric Company	Yes	
Electric Market Policy	Yes	On page 6, Table 2 Milestone Categories should indicate "months."

Organization	Yes or No	Question 11 Comment
Response: **The tables will be updated to reflect the time period as being in months.**		
PPL Corporation	No	PPL has concerns with the existing implementation schedule. Table 2 identifies some standard requirements as existing for Category 2 milestones. Having an Information Protection program does not mean that all information associated with a newly identified Critical Cyber Asset is immediately protected. For example, if an RE identifies an asset as critical with critical cyber assets, not all drawings and documentation will exist immediately marked as such. Even existing programs need to be applied to newly identified assets requiring an implementation schedule. The second concern is dependent on the outcome of the FERC Order for Clarification of CIP standards applicability to nuclear generating facilities. If the FERC Order results in nuclear facilities being included in the CIP applicability, this implementation plan should be noted to not include nuclear facilities affected by the pending FERC Order. The FERC Clarification Order needs to address the schedule for including nuclear facilities in the CIP applicability.
Response: **The SDT agrees with the example cited and will modify the Category 2 compliance time frame for CIP-003-2 Requirements R4, R5, and R6 to be 6 months.** **The issue of nuclear facilities is out of scope for this drafting team.**		
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	No	The 6 month implementation milestones listed for CIP-004-2 Category 2 should instead reflect 6 months from when the new security boundaries and systems get implemented instead of 6 months from the

Organization	Yes or No	Question 11 Comment
		identification of the newly identified Critical Cyber Asset. Entities will not be able to know all the affected personnel until the new physical and electronic security perimeters are defined and implemented.
Response: **The SDT agrees with the comment and will modify the timeframe to 18 months after the new CCA is identified for Category 2 for CIP-004 Requirements R2, R3 and R4.**		
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	The agreement would be based on the response to the CIP-004 background check requirement timeframe. The milestones would require adjustment for more exhaustive background checks.
Response: **Personnel can be granted unescorted access as long as a personnel risk assessment has been conducted according to the requirements in CIP-004 R3.** **A more exhaustive background check is not required; therefore an adjustment to the implementation plan is not necessary..**		
Orange and Rockland Utilities Inc.	No	1 - We recommend that Table 2 clarifies the units as months, per page 1 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.

Organization	Yes or No	Question 11 Comment
Response: **1) The tables will be updated to reflect the time period as being in months.** **2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
CenterPoint Energy		
Manitoba Hydro	No	CIP-003-2 R3, R4, and R5: The milestones should be changed to 6 months. Although the information protection, access control and change control and configuration management programs exist, the requirements also include implementation, which will require some time to meet compliance. CIP-008-2 R2: The milestone should be changed to 6 months, the same as R1. The documentation required in R2 is dependent upon the elements in the Cyber Security Incident Response Plan developed in R1. CIP-009-2 R2 and R3: The milestones should be changed to 6 months, the same as R1. The exercises and change control in R2 and R3 are dependent upon the elements in the Recovery Plan developed in R1.
Response: **The SDT interprets the comments to refer to Milestone Category 2.** **CIP-003, Requirement R3 has no implementation requirements, and thus the current timeframe is reasonable.** **The SDT will modify the Category 2 compliance timeframe for CIP-003-2 Requirements R4, R5, and R6 to be 6 months.** **The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
Alberta Electric System Operator		
Dynegy	Yes	

Organization	Yes or No	Question 11 Comment
Northern Indiana Public Service Company	No	I do not believe CIP-003-2 R3-R6 should be assumed to exist under Category 2 assets. An entity may need to identify exceptions, information, provide access control to that information and implement change control procedures on the newly identified asset. I also do not believe that it should be assumed that an entity can obtain the necessary financial capital to implement systems for compliance in any immediate fashion.
Response: **The SDT will modify the Category 2 compliance timeframe for CIP-003-2 Requirements R4, R5, and R6 to be 6 months.** **An entity that cannot comply within the implementation plan will be expected to submit a self-report of non-compliance with a mitigation plan that provides sufficient time to obtain funding.**		
CoreTrace		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	We interpret that the plan seems to collapse together the Compliant and Auditably Compliant milestones. We note that it is not possible to identify a new CCA, bring it into a state or Compliant (as defined in the currently applicable standard) and have one year of data and records as required to be Auditably Compliant. We believe clarification is required in this area.
Response: **The New Critical Cyber Asset Implementation Plan states that "the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the [compliant] milestone listed in this Implementation Plan."**		
American Electric Power	Yes	
Ontario IESO	Yes	We believe the proposed implementation plan is reasonable and appropriate.

Organization	Yes or No	Question 11 Comment
Response: **Thank you for your comment.**		
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1 - We recommend that Table 2 clarifies the units as months, per page 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Response: **1) The tables will be updated to reflect the time period as being in months.** **2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.		

Organization	Yes or No	Question 11 Comment
Progress Energy	No	The implementation plan for new CAs and CCAs allows 6-12-24 months for compliance, as noted by standard for Category 1-2 programs. For Category 2 programs (CIP program in place), for those requirements needing capitol funding anything less than 18 months would be difficult due to funding requests/process for capital. PE recommends those requirements potentially requiring significant capitol investment allowing a minimum of 18 months for compliance.
Response: **An entity that cannot comply within the implementation plan will be expected to submit a self-report of non-compliance with a mitigation plan that provides sufficient time to obtain funding.**		
Standards Review Committee of ISO/RTO Council	Yes	We believe the proposed implementation plan is reasonable and appropriate.
Response: **Thank you for your comment.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

12. The CSO706 SDT seeks input on whether to include the information contained in this **stand-alone implementation plan within the body of each standard.** This would likely entail a new requirement in CIP-002 to classify newly identified Critical Cyber Assets, and changes to the remaining standards to insert the milestone timeframes.

    Do you agree with including the information about newly identified Critical Cyber Assets and newly registered entity information within the body of the standards which would eliminate the stand-alone documents? If not, please explain.

Summary Consideration:

Organization	Yes or No	Question 12 Comment
Detroit Edison Company	Yes	
PacifiCorp	Yes	
FirstEnergy Corp	No	The stand alone document is sufficient and could be easily added as a reference document to each standard.
Response: **Thank you for your comment. The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	Yes	
WECC Reliability Coordination	Yes	
Southern Company	Yes	
Luminant Power	Yes	

Organization	Yes or No	Question 12 Comment
Encari	No	We agree that the requirement to identify new CCA should be included; however, we believe that a continued need to guide Responsible Entities in the selection of CAs and CCAs is still necessary as separate documents.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision. Guidelines for the identification of Critical Assets and Critical Cyber Assets are currently being developed.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	No	Including the implementation plan information in the individual CIP standards would greatly increase the size and complexity of each standard. All NERC Reliability Standards, including CIP, must be interpreted using various stand-alone documents (e.g., NERC Glossary of Terms Used in the Reliability Standards, NERC Reliability Functional Model, Compliance Monitoring and Enforcement Program, etc.). It's not a problem having the Implementation Plan available as a separate link or as a companion document to the CIP Reliability Standards.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Consolidated Edison Company of New York, Inc.	Yes	
Southern California Edison Company	Yes	
Tampa Electric Company	Yes	
Electric Market Policy	Yes	

Organization	Yes or No	Question 12 Comment
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates	Yes	In response to the CSO706 SDT question, we agree that the implementation plan for newly identified Critical Cyber Assets should be incorporated into the cyber security standard and believe that it should be included as part of CIP-002-1.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	I agree with including this information in the standards so everyone, user and Region, understands what is required. Leaving it in a stand alone document might allow for FERC to unilaterally change the implementation timeframe without stakeholder input. I hate to have to revise the CIP standards again, but this is important.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
City of Tallahassee (TAL)	Yes	I am for eliminating stand alone documents, although this incorporation can be made in Version 3, since you have stated one will be done for the more contentious issues.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will**		

Organization	Yes or No	Question 12 Comment
consider incorporating the implementation plan into the standards in a subsequent revision.		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	Inserting the information and time lines for newly identified Critical Cyber Assets and newly registered entity information into the body of the standards will cause unnecessary confusion regarding the implementation of the standards. By retaining the current stand-alone implementation plan it provides a ready reference and single point of information for all new Critical Cyber Assets and newly registered entities.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Orange and Rockland Utilities Inc.	Yes	
CenterPoint Energy		
Manitoba Hydro	Yes	Implementation plans which expire should be stand-alone documents from the standards. On-going implementation plans should be incorporated into the standards to create self-contained standards.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Alberta Electric System Operator		
Dynegy	Yes	

Organization	Yes or No	Question 12 Comment
Northern Indiana Public Service Company	Yes	
CoreTrace	No	To include the distinct procedures for newly identified Critical Cyber Assets would introduce a level of complexity and confusion into the current standard. As they stand today the CIP requirements are easy to understand and useful. A reference to the standalone implementation plan in the CIP body would be useful and sufficient and ensure that the information in the implementation plan was not overlooked.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation		
American Electric Power	Yes	AEP believes that there should be a statement in the standard providing a reference to the implementation plan and that the implementation plan be included in an appendix of the standard.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Ontario IESO	No	We believe that an implementation plan managed as a separate document is a more logical choice. Information is less likely to be repetitive and other standards can reference it as necessary. However, where an issue pertains to a single standard, it would be appropriate to include the pertinent implementation information within that standard.

Organization	Yes or No	Question 12 Comment
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	Yes	
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.		
Progress Energy	No	PE recommends referring to the implementation plan but not including it in the standard.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Standards Review Committee of ISO/RTO Council	No	We believe an implementation plan managed as a separate document is a more logical choice. Information is less likely to be repetitive and other standards can reference it as necessary. However, where an issue pertains to a single standard, it would be appropriate to include the pertinent implementation information within that standard.

Organization	Yes or No	Question 12 Comment
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
KEMA	No	Any change to the Standards is a long a laborious effort, so a change in implementation plan will have to go through the process. A separate document with the plan facilitites changes to the plan and not the Standard.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Austin Energy	No	I have a question as to why any newly installed asset would be anything but critical. Certainly existing assets can degrade to a point where they no longer fulfill a critical role, but why would a new asset be installed if there was not a need?
Response: **There may be multiple reasons for building a Bulk Electric System (BES) asset, including reliability or economic. Other reasons might include transmission to connect a new merchant generator (which may have economic benefit to the GO, but not necessarily the TO), or BES assets supporting increased retail or wholesale load. Alternatively, a parallel implementation to "modernize" a non-critical asset would still be non-critical. It is left up to the Responsible Entity to determine if the newly built asset is a Critical Asset based on its impact to the reliability of the BES. Similarly, a Cyber Asset might be installed within an Electronic Security Perimeter that is not determined to be a Critical Cyber Asset.**		
Kansas City Power & Light	Yes	This seems like the most logical place to put those requirements. Otherwise we'll end up with Standards that have to be cross-referenced against multiple sets of documents.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
San Diego Gas and Electric Co.	No	For clarity, SDG&E prefers the stand-alone Implementation Plan documents as presented rather than integrating the information for newly identified CCAs and newly registered entities into the existing CIP standards. This will help eliminate confusion and keep the existing Standard requirements and new

Organization	Yes or No	Question 12 Comment
		CCAs/Registered Entity information separate.

Response:

The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.

13. Do you agree that the Phase I improvements addresses the **time-sensitive FERC Order directives**? If not, please explain.

Summary Consideration:

Organization	Yes or No	Question 13 Comment
Detroit Edison Company	Yes	
PacifiCorp	No	The new effective date goes above the requirements listed in Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
Response: **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.** **The Standards Drafting Team believes that the six to nine month implementation plan is reasonable.**		
FirstEnergy Corp	Yes	For the most part we agree with the improvements except for our previous comments in questions 3, 10 and 11.Also, we offer the following additional suggested improvements:CIP-002-2 R3 - The phrase "automatic generation control" should be capitalized since it is a NERC defined term.CIP-003 M1 - The SDT should consider removing the second sentence "Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2" since the language in the first sentence already covers the necessary measure.CIP-005 R2.4 - The word "strong" should be removed since it is not clearly defined and measurable.CIP-007 - R2,R3,R5 - The word "establish" should be removed consistant with the other CIP standards. All that should be required is to "implement and document".- R5.1.2 - Replace "establish" with "have".- R7 - Replace "establish" with "document.CIP-009 - The first sentence in "Sec. B Requirements" which states "The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:" is not necessary and should be removed consistant with the other CIP revisions. FAQ Document - Is the SDT considering changes to the FAQ document to align with these proposed changed to the standards? Or is the FAQ document not a "living" document and was only to be used for the version 1 standards development? Regarding measures in CIP-002 through CIP-009, the drafting team should consider revising the measures to

Organization	Yes or No	Question 13 Comment
		include some guidance on the types of evidence or documentation that a responsible entity should and/or could have to demonstrate compliance. Throughout the standards the phrases "at least" and "at a minimum" are used and we fee that they are unnecessary. It is already understood that the standard requirements are the minimum expectations. Throughout the standards we suggest the SDT add the VRFs for each main requirement. Lastly, it would be appreciated if the SDT would use underlining in addition to the blue colored text to reflect inserted text for readability of black-n-white printed/copied material.
Response: **These types of issues will be addressed in Phase 2 of the CIP Standards; please use the Phase 2 comment period if you feel that your concerns have not been addressed.**		
MidAmerican Energy Company	No	The new effective date goes above the requirements listed in Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
Response: **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.** **The Standards Drafting Team believes that the six to nine month implementation plan is reasonable.**		
Northeast Power Coordinating Council	Yes	We agree with the removal of "reasonable business judgment" and "acceptance of risk".
Response: **Thank you for your comment.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	

Organization	Yes or No	Question 13 Comment
Luminant Power	No	Luminant thanks the Standards Drafting Team for their work addressing improvements to the NERC CIP Standards CIP-002 through CIP-009. As indicated by our "yes" responses to the comment form, in general Luminant agrees with the drafting team regarding the phased approach, implementation plan and the changes to address the time-sensitive issues from the FERC Order. However, on each standard the drafting team changed the language under the Data Retention sections 1.4.1 and 1.4.2. Luminant agrees with the intent of the changes but does not believe the language provides sufficient clarity. Luminant respectfully submits the following suggested language for the aforementioned data retention sections on each standard. 1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 for the current calendar year and the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation. The Responsible Entity shall keep documentation required by the Compliance Enforcement Authority for an investigation for one year after Compliance Enforcement Authority notice to the Responsible Entity that the investigation is completed.1.4.2 The Compliance Enforcement Authority and the Responsible Entity shall each retain all requested and submitted audit records from the most recent audit.
Response: **The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Encari	No	FERC provided directives on nearly all of the current requirements and guidance to include further requirements. The identification of what to modify in a time-sensitive manner was not open for public comment. We recognize the need to act swiftly to protect the assets; however, assurances also need to be made to protect system reliability. As an example, we feel that further clarifications around how to select critical assets and critical cyber assets would have provided a greater impact on the process and recommend that a public comment period be opened for the current draft guidelines. Therefore we recommend providing public comment periods to help the selection process of which FERC directives to introduce in the next phase of changes.
Response: **The Standards Drafting Team agrees that there are a variety of pressing needs such that a proritization process would be helpful. Once the time sensitive issues have been identified, the next step includes a discussion about the phased implementation approach**		

Organization	Yes or No	Question 13 Comment
to all of the FERC recommendations, while also considering industry needs.		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	Yes	We agree that Phase I addresses the time-sensitive FERC Order directives to remove "reasonable business judgment" and "acceptance of risk".
Response: **Thank you for your comment.**		
Southern California Edison Company	Yes	SCE hereby submits these additional general comments and questions (not related to or in response to Question 13): 1. What is the approval process for Violation Severity Levels? Will they be part of the standards? Will they be circulated for comment as part of the approval process? 2. In the Data Retention section of each Standard, a retention period is not specified for audit records. What is the retention period?
Response: **1) The Violation Severity Levels (VSLs) for Version 1 of the CIP Standards (CIP-002-1 through CIP-009-1) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team. The VSLs for Version 2 of the CIP Standards (CIP-002-2 through CIP-009-2) associated with the changes being proposed by the Standards Drafting Team for this project are currently being coordinated with the other Standards Drafting Team and will be posted for Industry Comment. The schedule for doing so is currently unknown.** **2) The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjuncgtion with" the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.**		

Organization	Yes or No	Question 13 Comment
Tampa Electric Company	Yes	
Electric Market Policy	Yes	
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	No	The new effective date goes above the requirements listed in Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
Response: **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.** **The Standards Drafting Team believes that the six to nine month implementation plan is reasonable.**		
Pepco Holdings, Inc - Affiliates	No	1. We understand that the SDT is proposing that Technical Feasibility Exceptions (TFE) Process (i.e. exception approval process) be modeled after the existing Self-Report and Mitigation Plan processes in the Compliance Monitoring and Enforcement Program (CMEP) which would require TFE review by the Regional Entity and NERC to assess the impact to the BES and then approve or not approve the exception. We also understand that as part of the NERC TFE approval process a mitigation plan would need to be submitted to the Regional Entity/NERC and completed for compliance. We understand that the Standards Drafting Team (SDT) is proposing that the TFE process be done through the NERC Rules of Procedure update process rather than through the standards process. Is it the intent of the SDT is to keep the TFE process outside of the compliance process (i.e., TFE requirement as part of the NERC Rules of Procedures)? 2. The existing Self-Report and Mitigation Plan process is for self-reporting and remedying a potential non-compliance. Is the intent of modeling the existing Self-Report and Mitigation Plan for the TFE process because the SDT considers Technical Feasibility Exceptions as non-compliance to the CIP standards? It was our understanding that TFEs are not a compliance issue. The existing FAQs state: Technical feasibility refers only to engineering possibility and is expected to be a "can/cannot" determination in every circumstance. It is also intended to be determined in light of the equipment and

Organization	Yes or No	Question 13 Comment
		facilities already owned by the Responsible Entity. The Responsible Entity is not required to replace any equipment in order to achieve compliance with the Cyber Security Standards. http://www.nerc.com/docs/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf 3. We believe that the TFE process needs to be included in the standards as well (e.g. CIP-003-2 R3). If the TFE is not coupled to the Standards (e.g. requirement to submit to RE and NERC for approval) we have concerns that there may be unintended gaps or conflicts. **(i)** For example what happens if a Registered Entity in following CIP-003-2 R3 (Exceptions) has a technical exception approved by the Sr. Manager but by a de-coupled TFE process NERC does not approve the exception? The Registered Entity is in compliance with the Standard but not with the TFE approval process. Would failure of a TFE procedure be considered non-compliance and therefore subject to fines? **(ii)** Another example of a potential gap or conflict is there could be conflicting effective dates of the standards and the TFE process (i.e. the requirement to submit to NERC for approval) if these are not linked together. **(iii)** Timing of the approvals by NERC could also create a gap or conflict. **(iv)** We encourage the SDT drafting team to consider including the requirement of RE/NERC review in the standards. The detailed process and procedures could be separate. **(v)** Finally we believe that the SDT needs to identify how the RE and/or NERC will perform the assessment of a TFE request on the impact to the BES (e.g. engineering judgement, load flow studies, stability studies,...) and identify the parameters that would be considered an approved exception versus an unapproved exception. 4. We understand and agree that NERC has the right to review TFE information and evidence of compliance but providing this information/data offsite may be considered a violation to the CIP requirement(s) and at the very least is a potential risk because if this information is compromised could show vulnerabilities to Critical Cyber Assets at a given Registered Entity. The confidentiality and security of the data/information needs to be considered. Potential options could include: • NERC could review information over a secure communication channel without NERC keeping the sensitive information

Organization	Yes or No	Question 13 Comment
Response: **1. The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.** **2. Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.** **3. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	I may not agree with all changes but they do address the FERC Order directives, even though by making these directives, they violate the ANSI approved process that they have stated NERC is required to follow.

Organization	Yes or No	Question 13 Comment
Response: **Comments regarding the ANSI process are outside the scope of the SDT to address.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	No	NIST Framework needs to be addressed NOW!
Response: **The Standards Drafting Team will consider the NIST risk management framework in future revisions of the standards.**		
US Bureau of Reclamation	No	The revisions are moving these standards away from "Critical Infrastructure Protection" towards "Cyber Infrastructure Protection." We believe this move strays from the original intent of Critical Infrastructure Protection as defined by the initial requirements. By focusing solely on the Cyber aspect, many important aspects of critical infrastructure protection will be lost. We reject any efforts to modify CIP from Critical Infrastructure Protection to Cyber Infrastructure Protection.
Response: **The Standard Drafting Team is focused on the cyber security aspects of critical infrastructure protection, a priority reflected in the SDT 706 SAR and driven by national security concerns about the adequacy of the industry's cyber security efforts as stated by Congressional Committees, FERC, and the new Obama Administration.** **Nonetheless, the SDT agrees that there is a critical need to address non-cyber critical infrastructure issues. If the commenter believes such an effort is warranted, we would recommend the submission of a SAR to specify the applicable issues.**		
Orange and Rockland Utilities Inc.	Yes	
CenterPoint Energy	No	See responses above to Q5, Q7, and Q8. In addition, the SDT changed the data retention wording in CIP-002 through CIP-009 such that "the Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records." CenterPoint Energy believes the retention time should be more defined and proposes adding

Organization	Yes or No	Question 13 Comment
		"until the next scheduled audit" to make it clear that data retention is on a rolling basis.
Response: **The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.**		
Manitoba Hydro	Yes	
Alberta Electric System Operator		
Dynegy	Yes	
Northern Indiana Public Service Company	Yes	Not sure if the question pertains to the CIP draft modifications or the proposed implementation schedule.
Response: **The Question pertains to both items.**		
CoreTrace		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation		
American Electric	Yes	As described above and following, AEP believes that there are a number of concepts that need to be

Organization	Yes or No	Question 13 Comment
Power		discussed and clarified in the standards. 1) AEP requests clarication be added about changes to Data Retention item 1.4.2. NERC reference materials suggest that the Compliance Enforcement Authority is solely responsible for keeping the last audit records. AEP does not believe that expanding the role of the Registered Entity, beyond that in any other standard, to include keeping audit documents is necessary or appropriate. However, there may be circumstances where confidential underlying data concerning critical infrastructure should only be retained only by the Registered Entity, but, even in such circumstances, auditing records should solely be retained under requirement by the Compliance Inforcement Authority. 2) Technical consideration should be given to determining the response to the "Compliance Monitoring Period and Reset Time Frame" section. The drafting team reference guide has suggested time periods aligning with audits cycles and less than monthly reset time frames. The response that it is not applicable does not appear consistent. 3) Lastly, item M1 under Measures has inadvertently dropped the "The" while the remaining M2 - M4 do contain "The" at the beginning of each sentence. In some of the following CIP standards, it is presented correctly, and, in others, it is not aligned within the M1 item.

Response:

1) The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.

The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.

The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.

2) The compliance monitoring period and reset timeframe were linked to an older version of the sanctions table, and have no relevance to the sanctions table currently in use. Until the Reliability Standards Development Procedure is updated, we cannot remove this heading from the standard template; until then all drafting teams are placing the phrase, "not applicable" under the heading, "Compliance Monitoring Period and Reset Time Frame" in the standard.

Organization	Yes or No	Question 13 Comment
3) The compliance staff assisted in developing a set of guidelines for developing measures and compliance elements in standards – and these guidelines do allow various data retention periods. **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	Yes	Would like to see a clarification on what is intended by phrase "shall make available" that is included in measures for each standard and whom an entity is supposed to make documents available to. The change from a three year retention for documents to a non-specific period will provide additional burden to the compliance process, since the region will have an arbitrary time length assigned per specific incident.
Response: **The phrase, "shall make available" means that the responsible entity must allow the Compliance Enforcement Authority to see the evidence. The evidence is made available to the Compliance Enforcement Authority** **The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.** **The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.**		
Consumers Energy Company	Yes	
Xcel Energy		
ISO New England Inc	Yes	1) - We agree with the removal of "reasonable business judgment" and "acceptance of risk."

Organization	Yes or No	Question 13 Comment
		2) - GENERAL COMMENT: As a general matter, NERC needs to explain how it plans on enforcing these standards. This is critical, because NERC is not defining what cyber-security practices are, in fact, acceptable. Therefore, if a company establishes a "high bar for its internal programs (e.g., training employees), and does not meet its own business practices, it can be fined by NERC. By contrast (and depending on how the standards are enforced) companies that set "low bars" for its internal programs will escape penalty. NERC could inadvertently, through its compliance and enforcement policy, incent companies to establish "lowest common denominator" practices.
Response: **1) The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.** **2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
Progress Energy	Yes	1) Overall comment - PE recommends the removal of "Reasonable business judgment" be replaced with the use of "good utility practice" as defined by FERC. 2) Overall comment - Section D – Data Retention – It is not practical to leave data retention period totally open ended at the sole discretion of the Compliance Enforcement Authority, there should at least be a capped limit, PE recommends a maximum of 3-years to allow time between audits.

Organization	Yes or No	Question 13 Comment
Response: **1) The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.** **2) The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.**		
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	No	While the Standards Drafting Team has done a great job overall incorporating many of the issues raised in FERC Order 706 FERC, there appears to be two issues identified by FERC in Order 706 that have not been addressed by the Standards re-write team in these first revisions. FERC Order 706 directed in Paragraph 88 that features such as enhanced conditions on technical feasibility exceptions and oversight of critical asset determinations for CIP-002 are too important to the protection of the Bulk-Power System to wait until the 2009-2010 time period for the process to start. But no substantial modifications for CIP-002 in these areas are included from the SDT. In addition, FERC Order 706, in Paragraph 90, also directed the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule. This doesn't appear to have been completed by the SDT as a first priority.

Organization	Yes or No	Question 13 Comment
Response: **In Paragraph 88, the Commission ordered revisions to the CIP standards not be delayed until completion of the Version 1 standards Implementation Plan, and specifically cited the CIP-002-1 and Technical Feasibility Exceptions (TFE) as priority revisions.** **The Commission at Paragraph 253 adopted the NOPR proposal requiring the ERO to provide additional guidance as to the features and functionality of an adequate risk-based assessment methodology, while leaving to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. The NERC Critical Infrastructure Protection Committee is in the process of developing specific Guidelines to address this requirement. The SDT believes the development of the Critical Asset and Critical Cyber Asset Identification Guidelines currently underway address the immediate concerns of the Commission. In addition, the SDT will be examining the entire risk management framework. Due to the complexity of this issue, the SDT decided to address risk management and its impact on CIP-002 early in Phase 2 in order to not delay the time-critical modifications directed elsewhere in the Final Order.** **The Commission at Paragraph 178 directed the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards. NERC Staff, with consultation with the SDT, has begun to develop a process for handling Technical Feasibility Exceptions (TFE) that is modeled after the existing self-report of non-compliance with mitigation plan process, as described in the NERC Rules of Procedure (ROP) Appendix 4C. The TFE process is not a "requirement" of a "standard" - it is a process for meeting requirements in standards. The TFE process is considered to be a compliance issue, although it is anticipated to be a way of being "compliant" with a standard in the event that an entity cannot meet the specific requirements of the standard. Because the TFE process is a compliance process, not development of requirements, it is outside the charter of the SDT. Therefore, the TFE process development and approval will be moving away from a direct SDT effort, to follow the established process for modifying the NERC ROP. As such, the SDT will not have a formal role in continued development of the process. The established ROP update process includes public comment and stakeholder input (including continued input from the SDT).**		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Modified Standards

The following standards have been modified:
CIP–002–2 — Cyber Security — Critical Cyber Asset Identification
CIP–003–2 — Cyber Security — Security Management Controls
CIP–004–2 — Cyber Security — Personnel and Training
CIP–005–2 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–2 — Cyber Security — Physical Security
CIP–007–2 — Cyber Security — Systems Security Management
CIP–008–2 — Cyber Security — Incident Reporting and Response Planning
CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets

Red-line versions of the above standards are posted with this Implementation Plan. When these modified standards become effective, the prior versions of these standards and their Implementation Plan are retired.

Compliance with Standards

Once these standards become effective, the responsible entities identified in the Applicability section of the standard must comply with the requirements. These include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

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

Newly registered entities must comply with the requirements of CIP-002-2 through CIP-009-2 within 24 months of registration. The sole exception is CIP-003-2 R2 where the newly registered entity must comply within 12 months of registration.

Proposed Effective Date

The proposed effective date for these modified standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters) after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.

Implementation Plan for Cyber Security Standards CIP-003-1~~2~~-2 through CIP-009-1~~2~~ or Their Successor Standards

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan identifies the schedule for becoming compliant with the requirements of NERC Standards CIP-003-1~~2~~ through CIP-009-1~~2~~ and their successor standards, for assets determined to be Critical Cyber Assets once an Entity's applicable 'Compliant' milestone date listed in the existing Implementation Plan has passed.

This Implementation Plan specifies only a 'Compliant' milestone. The Compliant milestone is expressed in this Implementation Plan table (Table 2) as the number of months following the designation of the newly identified asset as a Critical Cyber Asset, following the requirements of NERC Standard CIP-002-1~~2~~ or its successor standard.

For some requirements, the Responsible Entity is expected to be Compliant immediately upon the designation of the newly identified Critical Cyber Asset. These instances are annotated as '0' herein. For other requirements, the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date. These are annotated as *existing*.

In all cases where a milestone for compliance is specified (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the milestone listed in this Implementation Plan. Where the milestone assumes prior compliance (i.e., is annotated as *existing*), the Responsible Entity is expected to have all documentation and records showing compliance (i.e., 'Auditably Compliant') based on other previously defined Implementation Plan milestones.

There are no Implementation Plan milestones specified herein for compliance with NERC Standard CIP-002. All Responsible Entities are required to be compliant with NERC Standard CIP-002 based on the existing Implementation Plan.

Implementation Schedule

There are three categories described in this Implementation Plan, two of which have associated milestones. They are briefly:

1. A Cyber Asset becomes the *first identified* Critical Cyber Asset at a responsible Entity. No existing CIP compliance program for CIP-003 through CIP-009 is assumed to exist at the Responsible Entity.
2. An existing Cyber Asset becomes subject to CIP standards, *not due to planned change*. A CIP compliance program already exists at the Responsible Entity.
3. A new or existing Cyber Asset becomes subject to CIP standards *due to planned change*. A CIP compliance program already exists at the Responsible Entity.

Note that the term 'Cyber Asset becomes subject to the CIP standards' applies to all Critical Cyber Assets, as well as ~~non-critical~~other (non-critical) Cyber Assets within an Electronic Security Perimeter.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

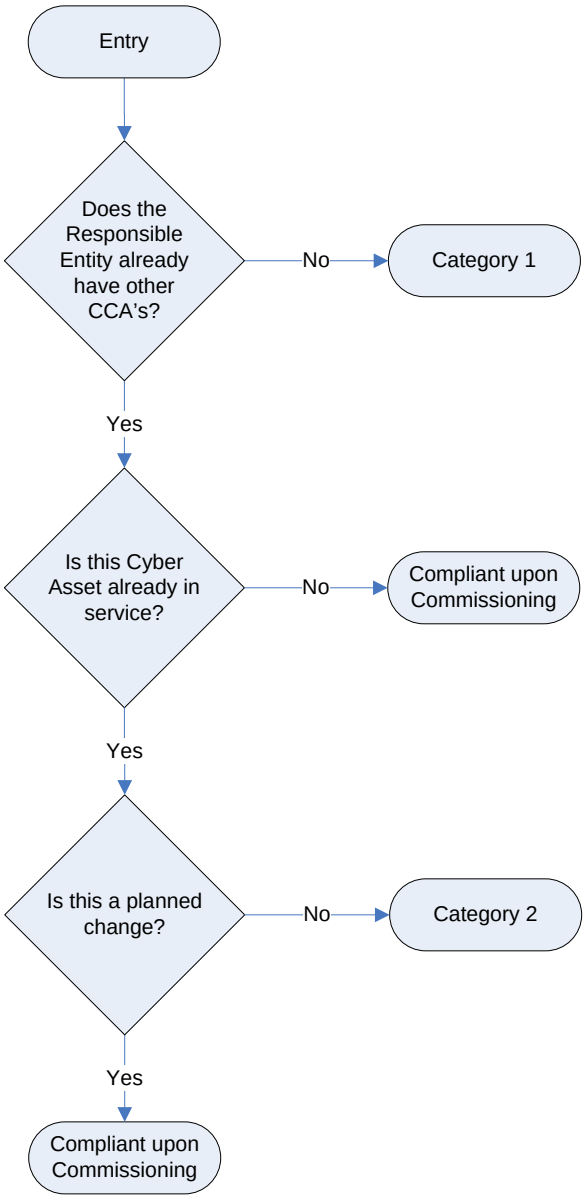

Figure 1: Category Selection Process Flow

The individual categories are distinguished as follows:

1. **Category 1**: A Responsible Entity that previously has undergone the CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. The Compliant milestone specified for this Category shall be the same as Table 3 of this New Asset Implementation Plan. (Note that Table 3 of this New Asset Implementation Plan provides the same schedule as was provided in Table 4 of the original Implementation Plan for Standards CIP-003~~-1~~-2 through CIP-009~~-1~~-2.) As such, it is presumed that the Responsible Entity has no previously established cyber security program in force. Table 3 also shall apply in the event of a Responsible Entity business merger or asset acquisition where previously no Critical Cyber Assets had been identified by any of the Entities involved.

2. **Category 2**: A Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule, and now has added additional items to its Critical Cyber Asset list. The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented. Since the Responsible Entity already has a CIP compliance program, it needs only to implement the CIP standards for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*, not when they are added or modified through construction, upgrade or replacement.

   In the case of business merger or asset acquisition, if any of the Responsible Entities involved had previously identified Critical Cyber Assets, implementation of the CIP Standards for newly identified Critical Cyber Assets must be completed per Compliant milestones established herein under Category 2. In the case of an asset acquisition, where the asset had been declared as a Critical Asset by the selling company, the acquiring company must determine whether the asset remains a Critical Asset as part of the acquisition planning process.

   In the case of a business merger where all parties already have previously identified Critical Cyber Assets and have existing but different CIP Compliance programs in place, the merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate programs and to determine how to either combine the programs, or at a minimum, combine the separate programs under a common Senior Manager and governance structure. At the conclusion of the one calendar year period, the Category 2 milestones will be used by the Responsible Entity to consolidate the separate CIP Compliance programs.

   A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

3. **Compliant upon Commissioning**: When a Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

    a) 'Greenfield' construction of an asset that will be declared a Critical Asset upon its commissioning or activation (e.g., based on planning or impact studies).
    b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security ~~perimeter~~Perimeter) associated with a previously identified Critical Asset.
    c) Planned a~~A~~ddition of:
        i. a Critical Cyber Asset, or,
        ii. an other (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter.

    In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset where that Entity has an established CIP Compliance Program as required by an existing Implementation Schedule.

    This scenario shall also apply for any of the above scenarios where relevant in the event of business merger and/or asset acquisition.

    A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

    A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

    Since the assets must be compliant upon commissioning, no milestones are provided herein.

Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards.

As an example, Table 1 provides some sample situations, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Program:	
	No CIP Program (note 1)	Existing CIP Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset - never before in service and not a replacement for an existing Cyber Asset - added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) ~~non-critical~~ asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	~~1~~*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	~~existing~~6 months
R5	24 months	6 months~~*existing*~~
R6	24 months	6 months~~*existing*~~
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18~~6~~ months
R3	24 months	~~6~~18 months
R4	24 months	~~6~~18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	~~0~~6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	~~0~~12 months
R3	24 months	~~0~~12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[1] Compliance Schedule for Standards CIP-002~~-1~~-2 through CIP-009~~-1~~-2 or Their Successor Standards For Entities Registering in 2008 and Thereafter				
	Upon Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	**All Facilities**	**All Facilities**	**All Facilities**	**All Facilities**
CIP-002~~-1~~-2 Critical Cyber Assets or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-003~~-1~~-2 — Security Management Controls or its Successor Standard				
All Requirements Except R2	**BW**	**SC**	**C**	**AC**
R2	**SC**	**C**	**AC**	**AC**
Standard CIP-004~~-1~~-2 — Personnel & Training or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-005~~-1~~-2 — Electronic Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-006~~-1~~-2 — Physical Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-007~~-1~~-2 — Systems Security Management or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-008~~-1~~-2 — Incident Reporting and Response Planning or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-009~~-1~~-2 — Recovery Plans or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**

[1] The phase in of compliance in this table is identical to the phase in for CIP-002-1 through CIP-009-1 identified in Table 4 of the 2006 CIP Implementation Plan.