

## Comment Form for Phase I of Project 2008-06 — Cyber Security Order 706

Please use the [electronic comment](#) form located at the link below to submit comments on the proposed revisions of CIP-002-1 through CIP-009-1, developed by the standard drafting team as part of Project 2008-06 — Cyber Security Order 706. Comments must be submitted by **January 5, 2009**. If you have questions please contact Harry Tom at [Harry.Tom@nerc.net](mailto:Harry.Tom@nerc.net) or by telephone at (860) 550-4157.

[http://www.nerc.com/filez/standards/Project\\_2008-06\\_Cyber\\_Security.html](http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html)

### Background Information

On July 10<sup>th</sup>, 2008, the NERC Standards Committee approved the Standard Authorization Request (SAR) for developing revisions to the following Critical Infrastructure Protection Cyber Security standards:

- 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

A Standards Drafting Team (SDT) was appointed by the Standards Committee on August 7, 2008 to develop these revisions as part of Project 2008-06 — Cyber Security Order 706. The SDT for Project 2008-06 has been assigned the responsibility to review each of the reliability standards identified above 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](#). In conjunction with the project, the SDT will also consider other cyber-related standards, guidelines and activities:

- The National Institute of Standards and Technology (NIST) Security Risk Management Framework [includes General Accounting Office (GAO), Office of Management and Budget (OMB) and Federal Information Processing Standards (FIPS)].
- Other cyber security related documents such as NIST, International Organization for Standardization (ISO) 27000 Family, Critical Infrastructure Protection Committee (CIPC) Risk Assessment Guideline, MITRE corporation technical report, Department of Homeland Security (DHS), National Laboratories papers, Department of Energy (DOE) 417, International Electrotechnical Commission (IEC), International Society of Automation (ISA), etc.
- Coordination work between FERC, Nuclear Energy Institute (NEI) and Nuclear Regulatory Commission (NRC) in regard to the nuclear facility exemption issue with respect to regulatory gaps and modify, as necessary, the standards to reflect current determinations.

Revisions will consider additional issues identified by stakeholders in the SAR comment process. Issues are listed in the SAR at [http://www.nerc.com/docs/standards/sar/SAR\\_Modify\\_CIP\\_Std\\_D2\\_clean\\_07Jul08.pdf](http://www.nerc.com/docs/standards/sar/SAR_Modify_CIP_Std_D2_clean_07Jul08.pdf) and [http://www.nerc.com/docs/standards/sar/SAR\\_Attach2\\_Order\\_706\\_Analysis.pdf](http://www.nerc.com/docs/standards/sar/SAR_Attach2_Order_706_Analysis.pdf) (two files).

The SDT met on October 6–8, 2008 and because of the extensive scope and varying complexity of the issues and work in these revisions, the team decided on a multiphase approach for revising this set of standards. This posting of the cyber standards for industry comment only relates to Phase I of the project.

### Summary of Phase I Revisions

Phase I 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 modifications and are outlined below. 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 of Project 2008-06 — Cyber Security Order 706.

The following provides a brief summary of the proposed modifications to this set of standards as Phase I of Project 2008-06 — Cyber Security Order 706. For All CIP 002-1—CIP 009-1 Standards the following modifications are proposed:

- As directed in Order 706
  - Purpose Section: Removed the term "reasonable business judgment".
  - Where applicable, removed the phrase "acceptance of risk".
- To comply with ERO Rules of Procedure
  - Applicability: Added Regional Entity in place of Regional Reliability Organization.
- Versioning
  - Phase I changes to the existing version will be reflected as CIP 002–2 through CIP 009–2.
- Effective Date section updated to integrate the implementation timeframe for CIP 002–2 through CIP 009–2.
- Administrative edits to reflect changes in numbering references.
- Requirements
  - Where there were sub-requirements that were numbered, but were not all required, the numbers were replaced with "bullets".
- Measures
  - The format of the measures was modified to conform to the format used in other standards.
- Compliance Elements
  - The compliance elements of the standard were updated to reflect the language used in the ERO Rules of Procedure.
  - The term, "Compliance Monitor" was replaced with "Compliance Enforcement Authority".

- The term, “Regional Reliability Organization” was replaced with “Regional Entity”.
- The Compliance Monitoring and Enforcement Processes were added.
- The Monitoring Time Period and Reset Periods were marked as “not applicable”.
- The Data Retention section was updated.

In addition to the changes noted above, the following modifications are proposed to apply to specific CIP standards as noted below:

**CIP 002 Modifications**

- As directed in Order 706
  - R4 Annual Approvals: Adds that the senior manager shall annually review and approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets as required in prior version.

**CIP 003 Modifications**

- Simplification
  - R2.1 Leader Identification: Removes the need for business phone and business address designation.
- As directed in Order 706
  - Applicability 4.2.3: Requires Responsible Entities having no Critical Cyber Assets to comply with CIP 003-2 R2.
  - R2 Leadership: Require the designation of a single manager, with overall responsibility and authority for leading and managing the entity's implementation of CIP. The word “authority” is an addition.
  - R2.3: Permits the assigned senior manager to delegate authority in writing for specific actions, where allowed, throughout the CIP standards.

**CIP 004 Modifications**

- Clarification to assure that requirement must be implemented
  - R1. Awareness: Explicitly requires implementation of Awareness Program.
  - R2. Training: Explicitly requires implementation of the Training Program.
- As directed in Order 706
  - R2.1 Training: Personnel having access to Critical Cyber Assets must be trained prior to their being granted such access, except in specified circumstances, such as an emergency. This replaces allowance for ninety days to complete the training and adds provision for emergency situations.
  - R3 Personnel Risk Assessment: Personnel risk assessment shall be conducted prior to granting personnel access to Critical Cyber Assets except in specified circumstances such as an emergency. This replaces allowance for thirty days to complete personnel risk assessment and adds provision for emergency situation.

**CIP 005 Modifications**

- Clarification
  - Clarifies the scope of this requirement to include Cyber Assets used in either access control and/or monitoring to the Electronic Security Perimeter.
- Clarification to assure that requirement must be implemented
  - R2.3 Electronic Access Controls: Explicitly requires the implementation of the procedure to secure dial up access to the Electronic Security Perimeter.

### **CIP 006 Modifications**

- Restructuring of Requirements
  - Former requirement R1.8 moved and incorporated into new Requirement R2 (Protection of Physical Access Control Systems) as Requirement R2.2.
  - Other modifications to Requirements R1.1 through R1.8 for readability.
- Clarifications to assure that requirement must be implemented
  - R1.–R1.8 Physical Security Plan: All requirements of the Physical Security Plan must be implemented.
- Additional Clarifications
  - R1.6 Escorted Access: Clarified that the escort within a Physical Security Perimeter should continually remain with the escorted person.
  - R1.8 Annual Review: Formerly Requirement R1.9.
  - R2.2: Formerly R1.8. Changed references to requirement numbers as appropriate.
  - R4 Physical Access Controls: Formerly Requirement R2. Changes enumeration of sub requirements to bulleted list.
  - R5 Monitoring Physical Access: Formerly Requirement R3. Changes enumeration of sub requirements to bulleted list. Changes references to other requirements as appropriate.
  - R6 Logging Physical Access: Formerly Requirement R4. Changes enumeration of sub requirements to bulleted list. Changes references to other requirements as appropriate.
  - Requirement R7: Formerly Requirement R5.
  - R8 Maintenance and Testing: Formerly Requirement R6. Changes references to other requirements as appropriate.
- As directed in Order 706
  - R1.7 Updates to the Physical Security Plan: Shortens the time for updates to the Physical Security Plan to thirty calendar days rather than ninety days and adds the word “completion” to the requirement.
  - R1 Physical security Plan: Changes the term “a senior manager” to “the senior manager.”
- Requirements Added
  - R2 Protection of Physical Access Control Systems: Moves requirement to protect Physical Access Control Systems out of Requirement R1 into its own requirement and excludes hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers from the requirement.
  - R2.1 Protection of Physical Access Control Systems: Adds requirement that Physical Access Control Systems be protected from unauthorized access.
  - R3 Protection of Electronic Access Control Systems: Adds that cyber assets used in access control and/or monitoring of the Electronic Security Perimeter shall reside within an identified Physical Security Perimeter.

### **CIP 007 Systems Security Management Modifications**

- As directed in Order 706
  - R2.3 Ports and Services: Removal of the term “or an acceptance of risk.”
  - R3.2 Security Patch Mgt.: Removal of the term “or an acceptance of risk.”
  - R4.1 Malicious Software Prevention: Removal of the term “or an acceptance of risk.”

- R9 Documentation Review and Maintenance: Shortens the time frame to update documentation in response to a system or control change from ninety to thirty calendar days and further clarifies this timeframe to begin after such change is complete.
- Clarifications to assure that requirements must be implemented
  - R2 Ports and Services: Explicitly requires the implementation of process to ensure only required ports and services are enabled.
  - R3 Security Patch Mgt.: Explicitly requires the implementation of Security Patch Management program.
  - R7 Disposal and Redeployment: Explicitly requires the implementation of Cyber Asset disposal and redeployment procedures.

### **CIP 008 Incident Response & Reporting Modifications**

- As directed in Order 706
  - R1.4 Updating the Cyber security Incident Response Plan: Shortens the timeframe to update the Incident Response Plan from ninety to thirty calendar days.
  - R1.6 Testing of the Incident Response Plan: Adds language to clarify that testing need not require a responsible entity to remove any systems from service.
- Clarifications to assure that requirements must be implemented
- R1 Incident Response Plan: Explicitly requires implementation.

### **CIP 009 Recovery Plan Modifications**

- As directed in Order 706
  - R3 Change Control: Shortens the timeframe for communicating updates to Critical Cyber Asset recovery plans from within ninety to thirty calendar days of the change being completed.

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

The CSO706 SDT proposes an implementation plan to address newly identified Critical Cyber Assets. 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.

### **Questions**

Your responses to the following questions will assist the SDT for Project 2008-06 Cyber Security Order 706 (CSO706 SDT) in finalizing the Phase I work for CIP-002-2 through CIP-009-2 relative to the proposed modifications summarized above. For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply.

**You do not have to answer all questions. Enter All Comments in Simple Text Format.**

*Insert a “check” mark in the appropriate boxes by double-clicking the gray areas.*

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.

Yes

No

Comments: The MRO NSRS believes that R4 is prescriptive in nature. The requirement tells how to accomplish, not what to accomplish. [further comments that point to other standards]

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.

Yes

No

Comments: 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 entity.

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.

3. 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.

Yes

No

Comments:

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.

Yes

No

Comments:

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.

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.

Yes

No

Comments:

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.

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.

Yes

No

Comments:

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.

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.

Yes:

No

Comments: 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.

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.

- Yes
- No

Comments:

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.

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.

- Yes
- No

Comments: \*\*\*[MEC]This effective date as written could move the compliance date for Gnerator Owner functions up 6 months from the previously published compliance schedule. MRO stakeholders 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. 1
Apr. 1- June 30	Apr.1
July 1- Sept. 30	July 1
Oct. 1- Dec. 31	Oct. 1

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.

Yes

No

Comments:

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.

Yes

No

Comments:

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.

Yes

No

Comments:

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

Yes

No

Comments: \*\*\*[MEC]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.

MRO NSRS members:

Neal Balu WPS  
Terry Bilke MISO  
Carol Gerou MP  
Jim Haigh WAPA  
Charles Lawrence ATC  
Ken Goldsmith ALTW  
Terry Harbour MEC  
Pam Sordet XEL  
Dave Rudolph BEPC  
Eric Ruskamp LES  
Joseph Knight GRE  
Joe DePoorter MGE  
Larry Brusseau MRO  
Michael Brytowski, Secretary MRO