

Unofficial Comment Form for Project 2008-06 — Cyber Security Order 706 Draft CIP-002-4 Informal Review

Please **DO NOT** use this form to submit comments. Please use the [electronic form](#) located at the link below to submit comments on the proposed CIP-002-4. Comments must be submitted by **February 12, 2009**. If you have questions please contact Joe Bucciero at joe.bucciero@gmail.com or by telephone at (267) 981-5445.

Background Information:

[FERC Order 706](#) directed NERC to develop modifications to the CIP Reliability Standards. Some of the modifications were straightforward. Other changes included in Order 706, such as modification to the scope of assets covered by the standard and consideration of the NIST framework, are more complex and require additional consideration. A Standards Drafting Team (SDT) was appointed by the NERC 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 CIP cyber security 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](#).

Due to the wide variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase strategy to revise the CIP Standards. The initial phase of the project modified the CIP Standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706. The SDT's work in this initial phase resulted in Version 2 of the CIP standards. The NERC Board of Trustees approved Version 2 of the CIP Standards on May 6, 2009. On September 30, 2009 the Commission approved Version 2 of the CIP Reliability Standards for FERC jurisdictional entities.

In addition to approving the Version 2 CIP Standards, the Commission directed NERC to make additional changes to two of the standards (CIP-006-2 and CIP-008-2), the associated implementation plan and to file the modified standards and implementation plan within 90 days. On October 7, 2009, the Standards Committee approved the Standard Authorization Request (SAR) for Project 2009-21 Cyber Security Ninety-day Response. Although the Commission directed changes to only two of the eight (CIP-002-2 thru CIP-009-2) reliability standards, conforming changes were necessary and were drafted for the remaining six CIP Reliability Standards (CIP-002-2 through CIP-005-2, CIP-007-2, and CIP-009-2) to correct the cross references within the set of standards. The initial ballot for CIP-002-3 through CIP-009-3, an implementation plan for Version 3 of the CIP standards, and a supplemental *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* was held from November 20 to November 30, 2009. A recirculation ballot was completed on December 14, 2009. The output of this work became Version 3 of the CIP Reliability Standards. Version 3 CIP standards were approved by the NERC Board of Trustees on December 16, 2009 and will be submitted to FERC for approval by December 29, 2009 in accordance with the FERC 90-day directive.

The Standard Drafting Team is now considering Version 4 of the CIP Reliability Standards, addressing the FERC Order 706 cyber security directed modifications that may require industry discussion. Four key principles are guiding the drafting team's work on these standards:

- Build on work already done to comply with Version 1 of the CIP reliability standards, including the industry's experience and investments
- Address the complex nature of the BES reliability functions and interconnected Cyber Systems, both within and between multiple organizations
- Provide Responsible Entities with reasonable flexibility in applying equivalent security controls on the basis of compensating controls, cyber system characteristics, and operating environment considerations
- Include all Cyber Systems with potential to adversely impact the reliability of the BES if lost, comprised, or rendered unavailable

The SDT initially focused on revising CIP-002 since it establishes the foundation for cyber security protection of the BES. The subsequent cyber security standards establish the baseline cyber security controls that must be implemented to protect the assets identified in CIP-002. The drafting team has prioritized its work in response to Commission and industry concerns regarding identification of assets in CIP-002-1. Work on the remaining cyber security standards is scheduled to begin in January 2010. Drafts of the new standards are anticipated to be posted for industry feedback by July 2010.

Summary of CIP-002 Modifications

A new approach is proposed in draft standard CIP-002-4 — Cyber Security — BES Cyber System Categorization. In collaboration with representatives of the Operating Committee and Planning Committee, the drafting team developed criteria for evaluating the potential level of impact on functions critical to the reliable operation of the BES. The criteria are organized in high, medium, and low BES impact categories. Responsible Entities apply the criteria to map their identified BES Subsystems to BES impact categories. For each BES Cyber System, Responsible Entities assign the highest impact level of the associated BES Subsystem(s).

The Cyber Security Order 706 Standard Drafting Team requests industry feedback on the initial draft of CIP-002-4 — Cyber Security — BES Cyber System Categorization. Industry feedback gathered will be used by the drafting team to refine the draft standard for formal industry review in March 2010.

***Please use the [comment form](#) to submit your final responses to NERC.**

Questions:

1. Do you agree with the definitions and adoption of the following new or revised terms for inclusion in the NERC Glossary: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact? If not, please supply and explain your proposed modification.

1.a. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data.

- Agree with proposed definition
 Disagree with proposed definition

Comments:

The MRO NSRS approached every question as if it were in a vacuum, attempting to answer the individual questions honestly without being persuaded by the remainder of the standard. This meant addressing the questions as written and including comments only in the appropriate areas. While we may agree with the individual questions being asked, we request that the SDT give particular consideration to our comments found in question 13, which details our thoughts on the overall approach of the CIP-002-4 draft standard.

1.b. BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

- Agree with proposed definition
 Disagree with proposed definition

Comments:

We feel the definition should not assume an adverse impact, as that is for the processes within the standard to decide. We propose "A Cyber System associated with the operation of a Bulk Electric System Subsystem".

1.c. Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.

- Agree with proposed definition
 Disagree with proposed definition

1.d. Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

- Agree with proposed definition

Disagree with proposed definition

Comments:

We feel the definition is ambiguous as written, and propose the following reworded definition for clarity:

BES generation plants, including the Facilities required to connect them to a transmission system. Generation units whose combined output could become unavailable due to loss or compromise of a shared generation Element or shared generation Cyber System shall be considered as a single Generation Subsystem.

We also would like a clarification of “shared” as we had disagreement just within our MRO NSRS group on what this term implied.

Regardless, the terms “generation plant”, “generation unit”, and “transmission system” should be defined in the NERC Glossary of Terms.

1.e. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Agree with proposed definition

Disagree with proposed definition

Comments:

We feel the definition is ambiguous as written, and would propose the following reworded definition for clarity:

BES transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements. Transmission lines or busses whose combined flows could become unavailable due to loss or compromise of a shared transmission Element or shared transmission Cyber System shall be considered as a single Transmission Subsystem.

We also would like a clarification of “shared” as we had disagreement just within our MRO NSRS group on what this term implied.

Regardless, the terms “transmission substation” and “transmission bus” should be defined in the NERC Glossary of Terms, and “transmission lines” should be replaced with “Transmission Lines” to remove further ambiguity.

1.f. Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations

- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing
- Coordination of BES restoration activities.

Agree with proposed definition

Disagree with proposed definition

Comments:

We feel the bullet "alarm monitoring and processing" should be removed, as this functionality should inherently be included as part of the other processes listed. In some instances, it is even directly redundant as written.

We also feel the terms "generation plants" and "transmission substations" should be defined in the NERC Glossary of Terms, and "transmission facilities" should be replaced with "Transmission Facilities" to remove ambiguity.

1.g. High BES Impact — BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable:

- they could directly cause, contribute to, or create an unacceptable risk of-
 - BES instability; and/or
 - BES separation; and/or
 - a cascading sequence of failures.

or

- in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of-
 - instability; and/or
 - separation; and/or
 - a cascading sequence of failures;

or

- could hinder restoration to a normal condition.

Agree with proposed definition

Disagree with proposed definition

Comments:

The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1.

1.h. Medium BES Impact — BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could:

- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES; or
- in a planning time frame, under emergency, abnormal, or restorative conditions,
 - directly affect the electrical state or the capability of the BES; or
 - directly affect the ability to effectively monitor and control the BES.

Agree with proposed definition

Disagree with proposed definition

Comments:

The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1.

1.i. Low BES Impact — BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could **not**:

- directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures.
- hinder restoration to a normal condition.
- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES;

Agree with proposed definition

Disagree with proposed definition

Comments:

The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1.

2. The Purpose of draft CIP-002-4 states, "To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES." Do you agree that CIP-002-4 accomplishes this objective? If not, please explain why and provide specific suggestions for improvement.

Agree

Disagree

Comments:

3. The proposed method of categorizing BES Cyber Systems is to categorize BES Subsystems based on the criteria in Attachment 1, then determining the BES Cyber Systems that have the potential to adversely impact the functions in Attachment 2 performed by those BES Subsystems. An alternative method could consist of inventorying all BES Cyber Systems that can affect the reliability functions in

Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1. Do you prefer the method proposed in the standard? If not, please provide specific suggestions for a preferred alternative method.

Prefer method proposed in the standard

Prefer alternative method of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1.

Comments: We agree with the method in principle, however, see answers to questions 8 and 12 for specific comments on Attachment 1 and 2 criteria.

4. Requirement R1 of draft CIP-002-4 states "As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems*.

1.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.

1.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1."

Do you agree with this requirement? If not, please explain why and provide specific suggestions for improvement.

Agree

Disagree

Comments:

We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose the following:

Each Responsible Entity shall categorize the BES Subsystems it operates by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems*.

We feel R1.1 is ambiguous as written, and would propose the following:

The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of its commissioning of any new BES Subsystem, its decommissioning of any existing BES Subsystem or its modification of any existing BES Subsystem that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days following the completion of the commissioning, decommissioning, or modification.

We also feel the term "Reliability Assurer" should be defined in the NERC Glossary of Terms.

5. Requirement R2 of draft CIP-002-4 states, "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem:

- 2.1 Description of the Generation Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies)
- 2.2 The Responsible Entity name
- 2.3 The BES impact categorization level"

Do you agree with this notification proposal and approach? If not, please explain why and provide specific suggestions for improvement.

- Agree
 Disagree

Comments:

We feel the introduction statement "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets," adds nothing to the requirement and should be deleted.

6. Requirement R3 of draft CIP-002-4 states, "As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows:
- 3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.
 - 3.2. For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."

Do you agree with this requirement of assigning the highest impact level of the associated BES Subsystems? If not, please explain why and provide specific suggestions for improvement.

- Agree
 Disagree

Comments:

We feel the introduction statement “As a step in assigning appropriate security controls for its assets,” adds nothing to the requirement and should be deleted.

Otherwise, we agree with the method in principle, however, see answers to questions 12 for specific comments on Attachment 2 criteria.

7. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Agree with VSLs

Disagree with VSLs

Comments:

We'll withhold comments on these sections until the standard is more set.

8. Attachment 1 to draft CIP-002-4 contains criteria for High, Medium, and Low BES Impact categories developed in collaboration with representatives of the NERC Operating and Planning Committees. Do you have any suggestions that would improve the proposed criteria?

Suggestions for improving proposed criteria:

We feel Attachment item 1.2 should include “for the Contingency Reserve Sharing Group” at the end of the statement to make the intent less ambiguous.

Under Attachment item 1.2, we also feel the term “Reserve Sharing Obligations” should be defined in the NERC Glossary of Terms.

Under Attachment item 1.3, we feel the term “Reliability must run units” should be defined in the NERC Glossary of Terms.

Under item Attachment 1.4, we feel this represents the same “one size fits all” approach that the *Guidance for the Electric Sector: Categorizing Cyber Systems* document claims to be trying to eliminate. In reality, not all blackstart Generation Subsystems listed in the Regional Restoration Plan carry the same weight, or have the same impact on the region, so it seems like a hierarchy should be developed within the standard for categorizing these units as either High BES Impact, Medium BES Impact, or Low BES Impact. We feel this hierarchy should be based on the size of the Generation Subsystem (similar to the delineation defined by CIP-002-4 Attachment 1, sections 1.1 and 2.1, but not at the same MVA levels), as well as the Generation Subsystem’s impact on the Regional Restoration Plan, such as if it has a role in cranking support for a nuclear plant.

Attachment Item 1.4 currently does not differentiate between a utility having numerous blackstart capable Generation Subsystems, where failure of multiple blackstart Generation Subsystems would not compromise their entire blackstart plan, or a utility with a single blackstart Generation Subsystem that is then essential to the success of their blackstart procedure. It seems a utility should be given consideration for having multiple blackstart Generation Subsystems, which makes their blackstart plan inherently more reliable.

Under Attachment item 1.5, to remove ambiguity we feel we should replace “switching stations” with “switching stations or substations”.

Attachment Item 1.6 currently does not differentiate between a utility having numerous Cranking Path options, or a utility with a single Cranking Path that is then essential to the success of their blackstart procedure. It seems a utility should be given consideration for having multiple Cranking Path options, which makes their blackstart plan inherently more reliable.

Under Attachment item 1.9, the lack of a definition for “essential” makes this statement ambiguous.

Under Attachment item 1.10, we propose to replace “in voltage collapse” with “in voltage collapse that would pose an unacceptable risk to the Adequate Level of Reliability of the BES”.

Under Attachment item 1.12, we propose to add “as determined through an engineering evaluation or other assessment method” to the end of this statement.

Under Attachment item 1.13, we propose to add “as determined through an engineering evaluation or other assessment method” to the end of this statement.

Under Attachment item 1.16, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided.

Under Attachment item 2.2, to remove ambiguity we feel we should replace “switching stations” with “switching stations or substations”.

Under Attachment item 2.4, the lack of a definition for “essential” makes this statement ambiguous.

Under Attachment item 2.5, we propose to add “as determined through an engineering evaluation or other assessment method” to the end of this statement.

Under Attachment item 2.6, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided.

9. Do you have suggested criteria for high, medium, or low impact categories for Load-Serving Entities, Transmission Service Providers, and Interchange Coordinators?

Suggested Criteria for Load Serving Entities:

We feel they should not fall under the applicability of this Standard.

Suggested Criteria for Transmission Service Providers:

We feel they should not fall under the applicability of this Standard.

Suggested Criteria for Interchange Coordinators:

We feel they should not fall under the applicability of this Standard.

10. Do you have suggested criteria for high, medium, or low impact categories for NERC and Regional Entities?

Suggested criteria for NERC and Regional Entities:

We feel they should not fall under the applicability of this Standard.

11. The SDT is considering including Distribution Provider and Reliability Assurer in the list of applicable Functional Entities. Do you have any comments regarding whether or not the CIP-002-4 Standard should apply to these Functional Entities?

Comments on adding Distribution Provider:

We feel this Standard should only apply to Distribution Providers that own/operate BES assets.

Comments on adding Reliability Assurer:

This is difficult to ascertain without knowing the formal definition of a Reliability Assurer. We feel these needs to be defined in the NERC Glossary of Terms.

12. Attachment 2 to draft CIP-002-4 contains functions critical to the reliable operation of the Bulk Electric System that serve as a basis for categorization criteria and the definition of BES Cyber Systems. Do you have any suggestions that would improve the proposed functions?

Suggestions for improving proposed functions:

In and of themselves, not all of these functions are critical to the reliable operation of the BES in all cases, so we propose an alternative title of "Functions Utilized for the Reliable Operation of Bulk Electric System Subsystems".

We would also appreciate if the Standard Drafting Team could provide the basis for including each of these items.

13. Do you have any other comments to improve the draft standard?

Other Comments not already provided in response to earlier questions:

We believe the intent of the current version of standard CIP-002-3 has a better security focus than the proposed version 4, and that the current version of standard CIP-002-3 should either be maintained, or combined with certain aspects of the version 4 proposal. The current version of standard CIP-002-3 identifies BES sub-systems that are critical to the reliability of the BES, and then proceeds to identify cyber systems critical to the operation of the BES sub-systems. It then goes one step further by differentiating between routable and non-routable connections to these cyber systems. We believe this differentiation is extremely important, since non-routable connections (or even better, eliminating connections wherever practical) are inherently more secure against, and limit potential damage from, remote attacks. This seems to be a straight forward and direct approach to securing the BES from cyber attack, and we do not see any reason to deviate, especially when you consider that version 4 appears to be migrating away from the core scope of protecting against remote cyber attacks.

If the concern is too much latitude in the current version of standard CIP-002-3, then the new Identifying Critical Assets and Identifying Critical Cyber Assets guidelines should be rolled in to the current standard as core requirements instead of references, assuring that all entities identify critical assets under a similar, Engineering study based assessment. Completely replacing the existing standard

with the entirely new approach of version 4 does not appear to be prudent, as it undoes much of the groundwork laid by the existing standard that directly addresses BES security, especially when the version 3 Identifying Critical Cyber Assets guideline is currently out for formal comment at the same time.