

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

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 Version 4 Standards and Implementation Plans. Comments must be submitted by **December 10, 2010**. If you have questions please contact Howard Gugel at howard.gugel@nerc.net or by telephone at (609) 651-2269.

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

Background:

In 2008, FERC Order 706 paragraph 236 directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address their concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) inter-dependency analysis.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the [FERC Order 706](#). The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-002-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order 706 directives. CIP-010 and CIP-011 were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT limited the scope of modifications to requirements in CIP-002 through CIP-009 as an interim step to address the more immediate concerns raised in FERC Order 706, paragraph 236. The approach to address the remaining FERC Order 706 directives continues to be developed.

The SDT believes the NERC Standards CIP-002-4 through CIP-009-4 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.

The draft standard *CIP 002-4 – Cyber Security – Critical Cyber Asset Identification* identifies BES Cyber Systems according to “bright-line” criteria associated with the impact on reliable operation of the BES. The “bright-line” criteria is contained in *Attachment 1 – Critical Asset Criteria* of CIP-002-4. The *CIP-002-4 Cyber Security - Critical Asset Identification - Rationale and Implementation Reference Document* provides clarifying notes and rationale of the SDT. The draft CIP-003-4 through CIP-009-4 standards include conforming changes to match the versioning of CIP-002-4.

On September 20, 2010, the SDT posted CIP-002-4 for a formal 45-day comment period. During the comment period, the team received 101 sets of comments, including comments from more than 200 different people from approximately 125 companies representing 9 of the 10 Industry Segments. Concurrent with the comment period, a ballot pool was assembled and the first formal ballot was conducted. For the ballot a quorum was achieved, and the weighted sector vote was 43.33% affirmative.

Based on the comments received, a few changes were made to CIP-002-4.

- The Applicability section was modified to include an exemption for nuclear facilities regulated by the Canadian Nuclear Safety Commission, and Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.
- In addition, the effective date was changes to eight quarters after regulatory approval, so that entities are not required to maintain two sets of approved Critical Asset lists and Critical Cyber Asset lists during the implementation plan.
- Requirements R1 and R2 were modified slightly to clarify that each list must be updated on an ongoing basis, but the review and approval need only occur annually. Conforming changes were made to the compliance section.
- Finally, significant changes were made to Attachment 1 to ten of the criteria. One criterion was deleted, which allowed entities to place items on the Critical Asset list at their discretion.
 - The criterion for control centers was split into three criteria to allow for differentiation in size for Balancing Authorities and Transmission Operators.

All of these changes were in response to comments received.

A separate ballot is being conducted for CIP-005-4, and if the proposed standard is approved it will be filed with CIP-003-4 to CIP-009-4. If the proposed CIP-005-4 is rejected, then the present CIP-005-3 will be modified with conforming changes and filed with CIP-003-4 to CIP-009-4. The team is continuing to work on subsequent cyber security standards that will establish impact levels and define associated cyber security controls at levels appropriate to their BES impact.

The Team is seeking industry feedback on this draft of CIP 002-4. The industry feedback will be considered by the SDT in determining if there is a need to make any additional changes to CIP 002-4 requirements and related documents.

The SDT has provided a form for industry participants to offer their comments on this draft of CIP-002-4.

Question

Your response to the following question will assist the SDT for Project 2008-06 Cyber Security Order 706 in finalizing the work for CIP-002-4 through CIP-009-4 relative to the proposed modifications summarized above.

1. When reviewing the changes to the proposed CIP-002-4 standard, do you believe that the proposed standard was responsive to feedback received and provides acceptable bright-line criteria for the determination of Critical Cyber Assets?

Yes

No

Comments: The MRO NSRS believes the SDT was responsive to much of the feedback received from the industry; however, we question whether these bright-line criteria as a whole are acceptable for determining Critical Cyber Assets. We believe the following criteria need to be adjusted as follows to properly address these areas:

Attachment 1, Criterion 1.4

We believe EOP-005-2, which defines the Transmission Operator restoration plan and related Blackstart Resource requirements, is ambiguous as to what actually constitutes a Blackstart Resource. For example, assume a plant has a 1 MW diesel engine that is used to start a 100 MW combustion turbine when the system is black. What is the Blackstart Resource, the 1 MW diesel engine or the 100 MW combustion turbine? To our knowledge, EOP-005-2 does not answer this question. Even at the regional restoration plan level, we believe many utilities are currently designating the 1 MW diesel engine as the Blackstart Resource under EOP-005-2, whereas others have designated the 100 MW combustion turbine. We realize this appears to be more of an issue with EOP-005-2, and not CIP-002-4. However, the effect of this EOP-005-2 ambiguity will be greatly magnified once CIP-002-4 begins using this same designation to identify critical assets, determining where an entity focuses their time and resources related to cyber security. For this reason, we believe the CIP-002-4 and EOP-005-2 SDT's must work together to clarify this designation, enabling us to apply the definition of a Blackstart Resource, and the related cyber security efforts, uniformly across the industry.

Attachment 1, Criteria 1.4 & 1.5

The APPA has identified an issue where criteria 1.4 and 1.5 end up requiring nearly all control centers to be identified as critical, even for small entities. The MRO NSRS recognizes this unintended consequence, and supports the following APPA comments:

"The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size.

EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets.

Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW).

Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size.

Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW).

In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets.

To address this problem, we propose the following edits to 1.4 and 1.5 shown in quotation marks:

"1.4. Each Blackstart Resource identified in the **RESTORATION PLAN FOR A Transmission Operator SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION.**

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource **(S) IDENTIFIED IN 1.4.** to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan."

This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical."

The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized.

While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project. (CIP-002-5 or CIP-010/011)"

Attachment 1, Criterion 1.10

If a generating facility that falls under the brightline of criterion 1.1 has numerous Transmission Facilities providing interconnections to the system, all of them would be

designated as critical under criterion 1.10, even if their loss does not result in the loss of at least 1500 MW of generation. To prevent this, we would propose rewording the criterion as follows:

“Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in **THE LOSS OF AT LEAST 1500 MW OF GENERATION ASSETS IDENTIFIED BY AN GENERATOR OWNER AS A RESULT OF ITS APPLICATION OF ATTACHMENT 1, CRITERION 1.1, OR** the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.3.”

Attachment 1, Criterion 1.13

We are concerned that as currently worded, this criterion could unintentionally designate multiple smaller, disparate systems with like settings as a “system” that performs automatic load shedding of 300 MW or more, assuming the total combined load shedding capability of the disparate systems exceeds 300 MW. To prevent this, we would propose rewording the criterion as follows to more closely match the old version:

“Each **COMMON** system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.”

Attachment 1, Criterion 1.15

Even if a small utility, as a joint owner, has control over only a small portion of a large plant that falls under the brightline of criterion 1.1, we are concerned that as currently written, the first sentence of criterion 1.15 would unintentionally designate this small utility’s control center as critical. To prevent this, we would propose rewording the criterion as follows:

“Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.3, 1.4, **OR USED TO CONTROL AT LEAST 1500 MW OF GENERATION AT ANY FACILITY IDENTIFIED IN CRITERION 1.1.**”