

Executive Summary of Consideration of Comments on CIP-002-4 – Categorization of Cyber Systems

A first draft of CIP-002-4 was posted in December 2009 for an informal comment period of 45 days ending in February 2010. The industry responded to the posting with more than 500 pages of comments from more than 90 entities. The following is a summary of comments received and the response, where applicable, from the Standards Drafting Team (SDT). Note that the drafting team made so many changes to the standard based on stakeholder comments that the team is proposing the revised standard be given a new number, “CIP-010.”

1. **Definitions.** 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.

Summary Response: A number of respondents’ comments indicated some confusion between the definitions of Cyber System and BES Cyber System. Many also commented that the definition of Cyber System was too broad. The SDT considered these comments, has removed the definition of Cyber System since it is not referenced in the standard, and has modified the definition of BES Cyber System to include some of the concepts in the original definition of Cyber System into a single definition for BES Cyber System.

Respondents also commented on the definitions of Subsystems (BES, Generation and Transmission), cited vagueness and suggested the use of terms already defined in the glossary and in wide use in the industry. The SDT reviewed the comments and agreed that the use of terms already defined and widely used in the industry will serve the same purpose. The definitions for Subsystems have been removed and the references in the standard use terms already defined in the NERC Glossary or in wide use by the industry and any additional clarifying terms in the standard where “subsystems” were previously used.

Many respondents commented that the definition of Control Center needed more specific bounds. The SDT has modified the definition to add more specificity.

There were many comments on the need for definitions for High, Medium and Low Impact, since these are already defined by the criteria in Appendix 1. The SDT reviewed them and has removed these definitions.

Many also commented on the absence of a “No Impact” category. It is the SDT’s opinion that the definition of BES Cyber Systems effectively removes Cyber Systems with no impact from the scope, and that a BES Cyber System has some level of impact, by definition.

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.

Summary Response: There were a number of comments related to the absence of consideration for how BES cyber systems are connected in the categorization process. After much discussion, the SDT agrees that network connectivity should be a consideration, but that it is more appropriate to be considered in the drafting of requirements or controls that apply to categorized BES Cyber Systems or their components.

There were comments that addressed the approach where inheritance from the BES Subsystem Impact level would result on the same level of impact for all BES Cyber Systems associated with the subsystem. The SDT has made substantial changes to the draft to allow entities to use any method to identify BES Cyber Systems (i.e. to start with an inventory of all BES Cyber Systems, or to start with BES Facilities and the BES Cyber Systems supporting their real-time operations), as long as all BES Cyber Systems are identified.

Many respondents noted in their comments that they can only evaluate the purpose if the requirements and controls are posted together. The SDT has considered these comments and is posting the new draft together with drafts of the requirements or controls.

The Purpose has been redrafted to reflect these considerations.

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.

Summary Response: Of the 93 responses for this question, 49 preferred the method in the initial posting, 37 preferred the alternative method, and 7 did not have a preference. Many respondents commented that simplified criteria were needed. Some respondents noted that the standard should provide flexibility to use either approach. One entity noted that both alternatives must be executed in a comprehensive approach. Another entity commented on using CIP-002-3 as a base, expanding to all BES assets and applying the list of asset types in R1.2. Eight entities suggested using an approach based mainly on connectivity and secondarily on control centers and others. Some entities noted that a preference cannot be made in the absence of the controls. One entity proposed a hybrid approach, using a BES impact approach to filter out low impact BES Subsystems, then switching to a BES Cyber System based approach and classify based on the span of control of these BES Cyber Systems. Others cited the matrix approach described in the concept paper.

The SDT considered all comments and has made substantial changes to the requirements in CIP-002-4 (now CIP-010-1) to allow an entity to use any approach to reach the goal of the final

categorization of BES Cyber Systems. The new requirements are drafted with more focus on the objective and desired outcome, rather than on the methodology or process.

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.

Summary Response: *Of the total of 93 respondents, many commented again on the need to know the impact of controls. A number of respondents commented on the requirement for the Reliability Coordinator (RC) to approve engineering analyses: these commenters noted that RCs should be removed from these criteria. Some suggested that the Planning Coordinator is better suited for that role. Others commented that criteria for evaluation of engineering analyses were needed and that approved engineering analysis methodologies should be published. Some suggestions were made to specify a blanket option for engineering analyses to all criteria.*

There were a number of comments on the requirement for update, many on the amount of time specified before a change in the electric system is reflected. There were comments about the vagueness of the concept of BES Subsystems, and about questions of joint ownership, since the requirements focus on asset ownership. There were also comments on the open ended nature of the word “any” in the requirement.

The SDT considered these comments and has made substantial changes to the requirements. With a direct BES Cyber System to criteria for impact approach, the traditional use of BES impact engineering analyses becomes unnecessary for the evaluation of BES Cyber Systems, nor does any widely used methodology exist for that purpose. The criteria is now be based on bright lines and the impact categorization based on that of the BES Cyber Systems on the functions provided by BES Facilities.

The requirement for reviewing the categorization is now a separate requirement and based on changes in the BES Facilities that the entity owns or operates. The update period has also been extended to 60 days.

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.

Summary Response: The SDT thanks all respondents who commented on this requirement. In consideration of the overall comments received, the more direct statement of the impact categorization of BES Cyber System makes the requirement for notification unnecessary. This requirement no longer exists in the revised draft of CIP-002-4 (now CIP-010-1).

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.

Summary Response: Respondents commented that attachment 2 (Reliability Functions) was overly broad and open-ended, and that the focus should be on real-time systems. Many commented on the potential absence of correlation between the impact level of the BES Subsystem and the impact of the associated BES Cyber Systems on the functions. Others commented that the categorization methodology should be similar to that described in the

concept paper. Some noted that risk should be considered, not just impact: many cited connectivity as a factor. Some commented that there should be a No Impact category.

In consideration of these comments, the SDT has made substantial changes to the requirements. The categorization requirement is no longer based on an inherited categorization based on the impact level of the BES Subsystem, but each BES Cyber System is categorized based on its impact on BES Facilities which perform reliability functions. The scope has been clarified: BES Cyber Systems in scope are those which impact real-time operations of the BES.

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.

Summary Response: *Many respondents found it excessive for all requirements to have a High Violation Risk Factor. Some commented on the difficulty of assessing what was missed in the categorized BES Subsystems or Cyber Systems. Some commenters noted that requirements must be made clearer to properly make the assessment of the VSLs. There were many specific suggestions for changes to the wording in the VSLs.*

The SDT has redrafted the VSLs based on the substantially changed requirements in the new draft and on existing VSL drafting guidelines. VRFs have been assigned to the redrafted requirements.

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?

Summary Response: *Many respondents commented on the need to have the draft of requirements and controls available for review in order to comment. Commenters also wrote that criteria could be boiled down to two metric: supply/demand mismatch and exceeding IROLs. Many comments questioned the basis of the bright line thresholds in the criteria. A number of comments questioned the use of gross nameplate values for evaluation of generation capability and cited the MOD-024 for rating of generation capabilities. One commenter stated that exceeding an IROL within the timeframe allowed by standards should not be High Impact. Commenters also questioned the use of the phrase "...leaving the station". Some entities asked whether Distribution Facilities supporting restoration and UFLS were in scope.*

In formulating the thresholds and bright-line criteria, the SDT used many sources, such as the threshold in the NERC Event Analysis categories, and various thresholds used in existing standards.

The criteria are now used to categorize BES Cyber Systems based on their impact on the functions performed by BES Facilities. In consideration of comments, the SDT has revised, consolidated and removed various criteria in the former attachment 1. Most notably, the bright line criteria for generation are now based on defined terms in the NERC Glossary and used in standards MOD-024 and MOD-025. Criteria duplicative with IROLs have been restructured as options where IROLs are not used, and other criteria have been clarified and corrected where

required. Periodic and time parameters have been added where there may be multiple criteria thresholds within a given time.

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

Summary Response: *The vast majority of respondents had no suggested criteria for these entities. In fact, most felt that these entities should not be included as responsible entities in this standard. Those that felt that they should be included added that it depended on whether they had BES Cyber Systems. Some expressed that the systems were covered under other REs (Distribution Providers, TOPs, BAs)*

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

Summary Response: *The only respondents that felt these entities should be included said that NERCNet was probably the only concern. Several felt that even NERCNet would not affect the BES.*

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?

Summary Response: *Most respondents felt that the Reliability Assurer could be excluded (pointing to the fact that the RA is not included in the NERC Glossary and confusion over how compliance for NERC and Regional Entities could be measured). Results for the Distribution Provider (DP) were mixed. Some felt that the DP could be excluded, since they did not involve facilities $\geq 100\text{kV}$. Some felt that the DP should be substituted for the LSE. Some were unsure how load shedding and Smart Grid would affect this standard. Some were very opposed, feeling this opened distribution up to FERC regulation.*

The SDT agrees that the Reliability Assurer can be excluded, especially now that there is no requirement that directly references Reliability Assurers. However, there are many criteria that can directly affect Distribution Providers, especially when considering the NERC registration criteria for Distribution Providers. Such attachment 1 criteria for Protection Systems and UFLS can directly affect DP's that have such systems that are relevant for BES reliability. Registration criteria also point out that DPs that also satisfy Load Serving Entity registration criteria should register as LSEs. The SDT has included DPs in the list of applicable Responsible Entities.

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?

Summary Response: *Many respondents reiterated that the focus for these functions should be cyber systems that support real-time operations. Many found issue with the "include, but are not limited to" section of the functions. Others commented that attachment 2 is confusing and*

should be eliminated. Comments were made about unintended reliability effects, citing blackstart units as high impact, and therefore could result in reduction of these units. Commenters also wrote that the examples should be moved to a guidance document. One commenter noted that attachment 2 has a wider application and does not belong in a CIP standard.

The SDT has clarified the scope of the functions and removed all the examples. The former attachment 2 is a necessary attachment to define the scope for BES Cyber Systems and the functions they support.