

## **Official Comment Form for Cyber Security Concept Paper: “Categorizing Cyber Systems — An Approach Based on BES Reliability Functions”**

Please use this form to submit comments and suggestions on the Concept Paper entitled ‘*Categorizing Cyber Systems: An Approach Based on BES Reliability Functions*’. This form should also be used to provide responses to the specific questions raised to address a selected set of issues that are being considered by the Cyber Security Order 706 Standard Drafting Team (Project 2008-06). As the concept paper is posted to gather feedback, not for industry approval, responses to comments will not be provided.

**Comments must be submitted by September 4, 2009.**

Please submit the completed form by e-mail to [sarcomm@nerc.net](mailto:sarcomm@nerc.net) with the following subject line: “**Categorizing Cyber Systems Comment Form**”.

Only comments and suggestions submitted in **Microsoft Word format** using this form will be considered. Redline changes to the document and email comments will not be accepted.

If you have any questions on the subject information, please contact Scott Mix at [Scott.Mix@nerc.net](mailto:Scott.Mix@nerc.net).





**Enter All Comments in the table below. *Red-line Changes to the document will not be accepted.* Please submit this form in Microsoft Word format only.**

**Instructions:**

- Provide the page, line number, and section reference for each comment (page and line numbers are provided in the review version of the concept paper).
- Provide a description (or explanation) of your comment in the Comment column.
- Provide your suggestion in the Suggestion column.

The Cyber Security Order 706 Standard Drafting Team (CSO706SDT) is particularly interested in your feedback on the issues presented in the questions below. The standard drafting team will consider your comments and suggestions in the development of the proposed revisions to the Reliability Standard CIP-002 — Cyber Security — Critical Cyber Asset Identification. As the concept paper is posted to gather feedback, not for industry approval, responses to comments will not be provided. The standard drafting team's intent is to refine the approaches presented in the concept paper, not to revise the paper. The standard drafting team expects to post the proposed revisions to CIP-002 — Cyber Security — Critical Cyber Asset Identification for industry comment by the end of this calendar year.

**Questions:**

1. Section C, BES Reliability Functions discusses a categorization approach based on reliability functions. Is the concept of categorizing by function instead of by asset clear? If not why?

No, it is unclear if the whitepaper is trying to replace CIP-002 Requirement 1.2. The proposed process in the whitepaper does not provide any additional clarity or value to the process that is currently in place in CIP-002.

Will the BES Subsystem criteria listed in Table 1 replace the risk-based assessment methodologies developed by individual entities? Will each entity be given the flexibility to develop their own BES Subsystem criteria? The whitepaper appears that it is also going to affect CIP-002 Requirements 2 and 3 as well.

2. In Table 1, the BES Reliability Functions listed in the “BES Function” column were not meant to be comprehensive. Are there any other functions we need to address and why?

No. However, much of the BES subsystem criteria are lacking the detail required to apply in practice without making numerous assumptions. Forcing compliance to a strict set of criteria will also result in the unnecessary classification of some subsystems as critical.

3. Does the methodology presented in Section D, Identification of BES Subsystems and Section F, Identification of BES Cyber Systems capture all of the systems that will need to be protected to achieve an acceptable level of reliability? What other issues need to be considered?

Yes.

4. Section E, Impact Mapping of BES Subsystems proposes that all identified BES subsystems be mapped into categories based on pre-defined criteria that reflect their impact on the reliability and operability of the BES. This mapping will be based on pre-defined criteria in the functions they provide or support, which determine the level of that impact. Do you agree with this approach, and if not, what alternative suggestion do you have?

No. It is unclear what value would be added by having multiple classifications.

5. Section E, Impact Mapping of BES Subsystems provides an example of three impact levels: High, Medium, and Low. What do you believe is the appropriate number of levels for impact mapping of the BES subsystems, and why?

No, two classifications are acceptable - critical or non-critical.

6. Section E, Impact Mapping of BES Subsystems: Do you prefer discrete thresholds or performance based criteria for mapping the BES subsystems (e.g. MW values as opposed to percentage of total generation)? Please explain.

Discrete thresholds appear to lend themselves to more consistent auditing.

7. Section G, Categorization of Cyber Systems describes how an entity determines the impact a specific cyber system has on its assigned BES reliability functions. Do you agree with this process as described in the concept paper? Please explain.

No, two classifications are acceptable - critical or non-critical.

8. Section H, Final Categorization of Cyber Systems Based on Overall Impact on the BES describes an example process of how an entity combines the BES impact mapping and Cyber System impact analysis to determine the overall impact a cyber system has on the BES. Do you agree with this process described in the concept paper? Please explain.

No. The approach adds complexity without providing a reliability benefit.

9. Section I, Defining the Target of Protection describes how an entity determines the set of cyber assets necessary to provide security assurance in the BES functions the cyber system performs. Do you agree with this process described in the concept paper? Please explain.

No. There are concerns about potential scope expansion of protected assets such as "third parties" and, communication networks, and possibly cyber assets that are not dial-in or network accessible, which are out of scope today per the standards, may be brought in scope.

There is not a question for section J External Cyber Systems but these are referenced in section I.

10. Provide your company's thoughts on applying different levels of protection (i.e., security controls) based on characteristics and impact categories of specific BES cyber systems (e.g., transmissions substations, generating plants, control centers) as discussed in Section K, Applying Security Controls to the Target of Protection, of the concept paper.

All assets within the same ESP need the same level of protection. Section H, which assigns the impact category, is not clear and does not contain enough information to support a conclusion on section K.

11. Section K, Applying Security Controls to the Target of Protection, of the paper introduces the concept of a library of security controls. What sources would you recommend the drafting team consider when developing a library of security controls for protecting categorized BES cyber systems? What specific challenges would you anticipate in implementing controls from among a library of security controls?

Inadequate information has been provided in regards to the library of security controls. The library of security controls needs to be developed before a recommendation can be formed.

The library of controls might be appropriate in a case by case application but a global application should not be made mandatory since every company has unique methodologies.





