

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 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.

Individual Commenter Information (Complete this page for comments from one organization or individual.)	
Name:	Carol Gerou
Organization:	Midwest Reliability Organization
Telephone:	651-855-1735
E-mail:	ca.gerou@midwestreliability.org

Group Comments (Complete this page if comments are from a group.)		
Group Name:	NERC Standards Review Subcommittee	
Lead Contact:	Carol Gerou	
Contact Organization:	Midwest Reliability Organization	
Contact Telephone:	651-855-1735	
Contact E-mail:	ca.gerou@midwestreliability.org	
Additional Member Name	Additional Member Organization	Region
Neal Balu	Wisconsin Public Service	MRO
Terry Bilke	Midwest ISO	MRO
Ken Goldsmith	Alliant Energy	MRO
Jodi Jensen	Western Area Power	MRO
Terry Harbour	MidAmerican Energy Company	MRO
Joe Knight	Great River Energy	MRO
Alice Murdock	Xcel Energy	MRO
Scott Nickels	Rochester Public Utilities	MRO
Dave Rudolph	Basin Electric Power Cooperative	MRO
Eric Ruskamp	Lincoln Electric System	MRO

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, the proposed process in the whitepaper does not provide any additional clarity or value versus the current process that is currently in place in CIP-002. It appears that the categorization approach would replace CIP-002 Requirement 1.

Section C does not appropriately apply the Adequate Level Of Reliability as listed in Section B.

The MRO NSRS believes the intent of the current version of CIP-002 standard has a better security focus than the

proposed concept paper and that the current version of CIP-002 standard should be maintained since this concept paper does not elaborate in Section A on the maximum value the industry will receive by switching to this next risk-based assessment methodology plus, in Section C of this concept paper, an impact assessment is mentioned but it was not described how this assessment will be accomplished. The current version of CIP-002 standard 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. This appears to be a straight forward and direct approach to securing the BES from cyber attack and MRO NSRS does not see any reason to deviate from this approach.

If the concern is too much latitude in the current version of the CIP-002 standard, then maybe the new risk assessment guidelines should be officially amended to the current standard, assuring that all entities identify critical assets under a similar engineering study based assessment. Replacing the existing standard with an entirely new approach does not appear to be prudent, as it undoes much of the groundwork laid by the existing standard that directly addresses BES security.

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?

This concept paper is confusing as well as this question. The concept paper indicates Table 1 only gives illustrative examples (see Section C) then in Section D this same table is suppose to indentify all BES Subsystems. Then this question here is looking for more illustrative examples. Perhaps the methodology should be reviewed to determine what is an essential BES function.

MRO NSRS believes that Table 1 needs to focus on essential functions critical to preventing cascading outages / large blackouts and should not include protecting for an “Adequate Level of Reliability”.

However, the proposed approach does not provide more clarity than providing more specific criteria for asset selection under the current approach in the standards. More specific details would be required under any approach. MRO NSRS believes spending time adding clarity and specificity to the current standard is more productive.

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?

The methodologies presented in Sections D and F do not capture all of the systems that will need to be protected since the Adequate Level Reliability criteria was not applied correctly. In Section F, the MRO NSRS agrees the full target of protection should be identified especially before considering other cyber system components; it's unclear what these other cyber system components would be since Section F introduces them but does not explain what these systems are.

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. FERC Order 672 says that standards should be clear and unambiguous.

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?

There is not enough description for the impact levels ("high", "medium", or "low") for the MRO NSRS to make a judgment on whether it's appropriate or not. No matter what categories are developed there should be a category with a clear distinction between assets that are considered critical or not. With the implication that the facilities deemed critical will receive a prescribed level of security. MRO NSRS believes the existing two classifications are sufficient - 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.

It would appear to be appropriate to use a discrete level to be consistent with the existing NERC Operating Reliability Events Categories and the Statement of Compliance Registry Criteria Revision 5.0.

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.

There is not enough description for the impact levels (“high”, “medium”, or “low”) for the MRO NSRS to make a judgment on whether it’s appropriate or not. No matter what categories are developed there should be a category with a clear distinction between assets that are considered critical or not. With the implication that the facilities deemed critical will receive a prescribed level of security. MRO NSRS believes the existing two classifications are sufficient - 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. It will result in a mis-allocation of resources to highly improbable or impossible events. The approach adds complexity without providing a reliability benefit. Misallocation of resources will decrease the reliability and safety of the BES creditable threats both cyber or non-cyber will not receive sufficient resources given that there are finite resources to allocate.

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 – MRO NSRS believes the concepts presented in the paper could cause significant scope creep resulting in the addition of components that previously were not required to be included, or were deemed non-critical given their limited or no impact onto the reliability of the BES.

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.

The MRO NSRS agrees that there needs to be protection but not enough information is provided to apply security controls.

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.

