When completed, email this form to: sarcomm@nerc.com

Note: an Interpretation cannot be used to change a standard.

Interpretation 2010-xx: Request for an Interpretation of [Insert Standard Number], Requirement Rx, for [Insert Name of Company]
Date submitted: March 3, 2015 (amended May 8, 2015)
Contact information for person requesting the interpretation:
Name: Steven Parker
Organization: Energy Sector Security Consortium, Inc (EnergySec)
Telephone: 503.621.8179
Email: steve@energysec.org
Identify the standard that needs clarification:
Standard Number (include version number): CIP-002-5.1 (example: PRC-001-1)
Standard Title: Cyber Security — BES Cyber System Categorization
Identify specifically what requirement needs clarification:
Requirement Number and Text of Requirement: R1 For brevity, only relevant parts of the Requirement and Attachment 1 (incorporated by reference) are quoted here. Requirement 1, subpart 1.2 states, "Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2 …" Attachment 1 is incorporated into the requirement by reference. Attachment 1, Section 2, Criterion 2.1 states, "Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." Clarification needed: With respect to the exclusion clause of Criterion 2.1 limiting applicability, should the evaluation be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems? Stated differently, does the phrase "shared BES Cyber Systems" refer to discrete BES Cyber

Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Discussion

Criterion 2.1 introduces the concept of "shared BES Cyber Systems", but it is not clear what is meant by "shared". Additionally, Criterion 2.1 refers to such shared systems in the plural, making it unclear whether the intent was to apply the Criterion to groups of BES Cyber Systems, or simply to indicate that a single generating plant location could have multiple BES Cyber Systems that meet the Criterion.

Further adding to the uncertainty with this requirement are statements made within a NERC Lessons Learned document, "Impact Rating of Generation Resources", dated September 2, 2014. For example, the Lessons Learned document states:

> "If, for instance, the generation units and BES Cyber Systems are connected in a manner that could result in the loss of 1500 MW or more if **one or more** BES Cyber Systems at the plant were compromised or misused, then those shared BES Cyber Systems at the plant (i.e., those that can, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW) must be categorized as medium impact BES Cyber systems." (emphasis added)

In particular, the use of the phrase "one or more" suggests that a collective evaluation is required.

The aforementioned Lessons Learned document also states:

> "If a Responsible Entity adopts the segmentation approach, consistent with criterion 2.1, entities must provide evidence that BES Cyber Systems associated with any group of generating units at generating plants greater than 1500 MW are segmented effectively such that there are no **common mode vulnerabilities** that could result in the loss of 1500 MW or more of generation at a single plant." (emphasis added)

The reference to "common mode vulnerabilities" suggests that BES Cyber Systems should be evaluated as a group in some circumstances, but is unclear as "common mode vulnerabilities" is not a defined term.

The Lessons Learned document also states:

> "For example, Responsible Entities should consider physical locations that could present a single point of failure (e.g., common control rooms for multiple generating units) to determine what physical protections are appropriate."

Again, this language suggests that BES Cyber Systems may need to be evaluated in groups, for example, when multiple BES Cyber Systems are physically co-located.

The Lessons Learned document also contains a flow chart outlining a suggested process for evaluating BES Cyber Systems for impact ratings. That flow chart does not contain a process for grouping BES Cyber Systems for a collective evaluation, therefore suggesting that the impact assessment occurs individually for each discrete BES Cyber System.

A final Lessons Learned document was posted on January 29, 2015. Some of the language referred to above was removed in the final version, but the questions still remain. The final Lessons Learned document maintains the reference to the Guidelines section of the standard that refers to "BES Cyber Systems with common mode vulnerabilities". This

suggests that common mode vulnerabilities are evaluated in the context of groups of BES Cyber Systems.

In addition, the final Lessons Learned provides only two options, protecting all BES Cyber Systems at the medium level, or segmenting the units. The suggested evidence includes references to network segmentation and firewall rules. This suggests that for collections of BES Cyber Systems on a common network, the collective impact would be evaluated rather than their individual impact. Network isolation would be required to avoid this collective analysis.

On the other hand, FAQ 49, released for comment on April 1, 2015, states that a shared BES Cyber System is one that "affects two or more BES Facilities, such as multiple generation units." Likewise, FAQ 50 refers to common mode vulnerabilities as "Any systems that can affect two or more BES Facilities, such as multiple generation units. … Protection systems, fuel-handling systems, cooling water, and air systems are also examples that should be evaluated as common mode vulnerabilities." These responses support an assertion that BES Cyber Systems need only be evaluated individually.

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

The evaluation of BES Cyber Systems and assignment of impact ratings is a foundational requirement in version 5 of the CIP standards. A clear understanding of the Criteria, and their proper application is essential to ensure BES Cyber Systems are correctly rated so that the appropriate controls can be applied. Furthermore, in this case, confusion regarding a potential collective assessment, and the criteria and process for such an assessment, can lead not only to under or over rating of systems, but also significant expense in re-engineering plant systems and/or security controls.

A proper understanding of this Criterion is critical to ensure entities can comply with CIP-002-5 R1 without undue risk or expense.

Version History

Version	Date	Owner	Change Tracking
1	April 22, 2011		
1	May 27, 2014	Standards Information Staff	Updated template and email address for submittal.