Unofficial Comment Form for SAR and Proposed Modification to CIP-005-3 (Project 2010-15)

Please DO NOT use this form to submit comments. Please use the electronic comment form located at the link below to submit comments on the SAR and proposed modification to CIP-005-3 – Cyber Security – Electronic Security Perimeters (Project 2010-15). The electronic comment form must be submitted by April 28, 2011.


If you have questions please contact Scott Mix at Scott.mix@nerc.net or by telephone at 215-853-8204.

Background Information

Recent discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of large electric sector entities, necessitate expedient changes to industry security control standards.

Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter) can or should be accomplished. This expedited action will provide a (set of) mandatory and auditable requirement(s) for configuring secure remote access to Cyber Assets and electronic access control points (and other non-critical Cyber Assets within a defined Electronic Security Perimeter).

A supplementary guidance document (Secure Remote Access) recommends actions and best practice use-cases of in-place implementations to show how secure remote access may be implemented by a Responsible Entity and is also posted for stakeholder review.

1. Do you agree that there is a reliability-related need to modify CIP-005 – Cyber Security – Electronic Security Perimeters, to provide additional requirements for Cyber Assets used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter) from outside their Electronic Security Perimeter?

☐ Yes
☒ No

Comments: These Cyber Assets are currently outside of the scope of the CIP-002 - CIP-009 standards. Adding them only into CIP-005 raises concerns when accounting for related requirements in other CIP standards.
2. Do you agree with the proposed local definitions for "interactive remote access", "support or maintenance" and "intermediate device"?

☐ Yes
☒ No

Comments: Clarify “local definitions”, and where they are documented in the NERC Standards Process. Definitions are not clear and too broad. Define “support or maintenance” along with “operational” and “non-operational”.

“Intermediate device” appears to be too prescriptive. Requirement needs to be flexible for the various existing solutions. Need a clearer definition of “Intermediate device”.

R2.4 should be moved under R6. Is “Electronic Access” the same as “Interactive User Access”? If it is, then why is an additional definition for “User Interactive Access” necessary?

If it is not the same, then Identification and Authentication Controls should be moved under R6, as it pertains to IA controls for users/personnel. Electronic Access Controls would be for ports and services for device to device communication which currently, under CIP-005-3, do not require Identification and Authentication Controls.

CIP-004 R4 (cited under R2.4) only applies to personnel access authorizations, not device to device communication.
3. Do you agree with the proposed revisions to CIP-005?

☐ Yes
☒ No

Comments: This version is confusing, obscures any existing intent for security provisions of CIP-005-3, and adds no value to compliance or security initiatives.

R6.2 conflicts with the requirement for an Intermediate Device to be the endpoint of encrypted communication. In addition, where is the requirement for encrypted communications within an Entity’s site? If a user uses a cyber asset within an entity’s owned and controlled site there is no requirement to encrypt data communications. In that example the Intermediate Device is required to be the endpoint for encrypted communications when there is no requirements to encrypt data.

R6.3--appears to be too prescriptive for time-sensitive, multi-factor authentication architecture.

R6.4--If the cyber asset initiating the remote connection is NOT defined as a CCA/non-critical Cyber Asset then why are there requirements for anti-virus and patching which are consistent with CIP-007? CIP-007 directly applies to CCAs and non-critical Cyber Assets.

Agree that 6.4.2 and 6.4.3 are good corporate policy, but the initiating device may not fall under the CIP standards.

4. Are there any remaining “double-jeopardy” issues in the revised CIP-005?

☒ Yes
☐ No

Comments: R6 covers interactive user requirements and R2.4 should be merged into R6 to avoid double jeopardy.

Local definitions create potential for double jeopardy.

5. Do you agree with the proposed implementation language (tying the implementation timeframe to the filed Version 4 plan)?

☐ Yes
☒ No

Comments: NERC standard implementation requires eight quarters post approval.

6. If you have any other comments related to the revisions to CIP-005 to address securing remote access that you have not already provided in response to the questions above, please provide them here.

Comments: