

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 **December 11, 2010**.

http://www.nerc.com/filez/standards/SAR-Urgent_Action_Revisions%20to%20CIP-005-3.html

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-005-3 – 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:

2. Do you agree with the proposed revisions to CIP-005-3?

Yes

No

Comments: The clarifications made in R6 regarding the definition of "Remote Access" were a large improvement over previous revisions.

3. Do you agree with the proposed implementation language (six months to comply with the new Requirement R6 after the standard becomes effective)?

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

Yes

No

Comments: If an entity has remote substations designated as Critical Assets, 6 months does not provide ample time for research into technologies, re-design of the substation automation networks, and installation and testing. If this were only applied to EMS/SCADA systems at control centers, 6 months would be adequate. However, when entities are faced with long travel routes to and from remote substations, and that same travel is again required for troubleshooting, 6 months does not provide a reasonable implementation period for the new requirements placed on entities in R6 (installation of proxy servers, remote access systems, and new access controls). Recommend 18 months. Reasons for additional lead time would be to get asset ordered and budget approvals, installation of the asset, and to make sure the asset meets CIP requirements.