NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

When completed, email this form to:
maureen.long@nerc.net
For questions about this form or for assistance in completing the form, call Maureen Long at 813-468-5998.

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

Request for an Interpretation of a Reliability Standard

Date submitted: 11-4-10

Contact information for person requesting the interpretation:

Name: Gregory J. Ramon

Organization: Tampa Electric Company

Telephone: 813-228-4469

E-mail: GRamon@tecoenergy.com

Identify the standard that needs clarification:

Standard Number (include version number): CIP-007-1, CIP007-2, CIP-007-3
(example: PRC-001-1)

Standard Title: Cyber Security – Systems Security Management

Identify specifically what requirement needs clarification:

Requirement Number and Text of Requirement: R5.3

CIP-007-1, CIP007-2, CIP-007-3 Requirement R5 states:

> The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

CIP-007-1, CIP007-2, CIP-007- Requirement R5.3 states:

> At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
> R5.3.1. Each password shall be a minimum of six characters.
> R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.
> R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

Clarification needed:

CIP-007 R5 is being be interpreted inconsistently across Regional Entities as well as Registered Entities. One interpretation of this requirement and its sub requirements holds belief that an automated/technical solution is required for compliance with the Reliability Standard. However, as is evident from the use of the "technical and procedural controls" terminology set forth by NERC, procedural (*i.e.*, manual) controls are used when a technical solution is not possible or desirable. For example, CIP-005-1 R2 states that "The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access [to the Electronic Security Perimeter]". Likewise, CIP-005-1 R2.4 states that "the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible."

As is explained in the CIP FAQs, technical mechanisms relate to software or system controls, while procedural mechanisms are "manual processes and procedures that must be implemented for the electronic access controls to be effective." (CIP FAQs p. 14 Question 8). The use of procedural controls fits this description well. Manual procedures are used to ensure that adherence to the technical aspects of password complexity are enforced. In addition, the CIP FAQs go on to explain that "Procedural controls are often used to compensate for deficiencies in technical controls." This is precisely how Registered Entities have made use of procedural controls. Where technical controls are not practical or possible, Registered Entities have implemented manual controls to ensure that the Registered Entity remains compliant.

Other Reliability Standards with this phraseology also indicate that when this phrase is used either manual procedures or technical procedures may be employed. Registered Entities need not always use technical methods as indicated by some of the Regional Entities. For example, CIP-006-1 Requirement R3, which requires the implementation of "technical and procedural controls for monitoring physical access" to the Physical Security Perimeter (PSP), allows the use of automated alarm systems or manual observation of access points. Likewise, CIP-006-1 Requirement R4, which requires the use of "technical and procedural mechanisms for logging physical entry" to the PSP, allows the use of computerized logging or manual logging. Given that these Standards with the same language permit compliance through the use of a manual procedure rather than requiring automation, some entities are interpreting CIP-007-1 R5 inconsistently with the remaining body of approved CIP Reliability Standards.

This is particularly evident in interpretation and compliance with sub-requirement CIP-007-1 R5.3, as it relates to password controls and password complexity. Many cyber assets and critical cyber assets cannot technically enforce this requirement. In those instances, Registered Entities have implemented procedural controls to ensure that complex passwords are created and passwords are changed in compliance with this requirement. Given the available technology for these systems, this could be considered the norm within the industry as opposed to an exception.

We request an interpretation as to whether procedural controls are an acceptable method of complying with this requirement when enforcement cannot be achieved through technical means, or if BOTH technical and procedural controls must be implemented in every instance.

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.

If CIP-007R5 requires that only automated/technical solutions (“technical controls”) can be used to meet this requirement, a negative impact to the reliability of the Bulk Electric System may occur if procedural controls aren’t accepted as viable means to enforce password complexity. Particularly, instances when enforcement cannot be achieved through technical controls. Many cyber assets and critical cyber assets cannot technically enforce this requirement. Per the NERC CIP FAQs, "Procedural controls are often used to compensate for deficiencies in technical controls." (CIP FAQs p. 14 Question 8). If both technical and procedural controls are required, this could result in an excessive reporting requirement to be reviewed by the Regional Entities, FERC, and NERC based on the prevalent lack of electronic controls devised to enforce specifically to these requirements. Likewise, a lack of clarification may lead to possible non-compliance due to inconsistent interpretation.