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: 12-28-2011

Contact information for person requesting the interpretation:

Name:	Charles Lewis
Organization:	ITC Transmission
Telephone:	248-946-3182
E-mail:	clewis@itctransco.com

Identify the standard that needs clarification:

Standard Number (include version number): 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. Account Management — 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.

R5.3. 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:

ITC respectfully requests an interpretation regarding the following:

1. Does each sub-requirement, including R5.3, of R5 require that both "technical and procedural controls" be utilized?

2. Do "technical controls", utilized in the context of R5.3, mean that each individual cyber asset device within an ESP has to automatically enforce each of the three R5.3 sub-requirements? The three bullets below are part of this question; they are examples if this is interpreted to be true.

- R5.3.1. Each password shall be a minimum of six characters. Each individual cyber asset device within an ESP has to automatically reject any password that does not conform to a minimum of six characters.
- R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters. Each individual cyber asset device within an ESP has to automatically reject any password that does not conform to 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. Each individual cyber asset device within an ESP has to automatically force passwords to be changed at least annually or at a specified interval based on risk.

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 it is interpreted that R5.3 requires "technical controls" that automatically enforce password requirements, then there will be a need for entities to file a significant number of additional TFEs. The majority of devices used in the industry, while allowing passwords that meet all of the R5.3 sub-requirements, are not able to automatically enforce the requirements of R5.3.1, R5.3.2 and R5.3.3. In addition, it is expected the TFEs submitted for this requirement will have to be kept in place for a long period of time until device manufacturers create products that can enforce R5.3.1, R5.3.2 and R5.3.3.

A correct interpretation is needed for entities to determine whether existing cyber assets within ESPs are fully compliant with this requirement to avoid penalties associated with noncompliance.

Question

ITC Transmission seeks clarification on the meaning of CIP-007-3, Requirement R5 as it relates to both technical and procedural controls.

In its response, the Interpretation Drafting Team will answer:

1. Whether each sub-requirement of R5 requires both "technical and procedural controls."
2. Whether technical controls in Requirement R5.3 mean that each individual Cyber Asset within the Electronic Security Perimeter (ESP) has to automatically enforce each of the three R5.3 sub-requirements.

Response

Question 1: Does each sub-requirement of Requirement R5 require use of <u>both</u> "technical and procedural controls"?

No, it is not necessary for both technical and procedural controls to be used in each sub-requirement of Requirement R5. The use of "and" in Requirement R5 indicates that the responsible entity must implement both technical and procedural controls to achieve collectively the sub-requirements within Requirement R5 and the associated sub-requirements. Both are not necessary for each sub-requirement individually. Generally, technical controls are carried out or managed by computer systems. That is distinct from a technical aspect that enables or confirms procedural enforcement. While it is possible to have a technical component, tool, or aspect for each procedural control, mere use of technology to enable or support a procedural control is not necessarily a technical control itself. If a control relies on ongoing human intervention, then it is generally a procedural control. Procedural controls are the actions that people take, and they are the process of developing and ensuring compliance with policy and procedures. The responsible entity must look at what's performing the control to determine whether it's technical or procedural: the control is accomplished either by a human being using technology (procedural) or a computer managing or performing the control (technical). The IDT also notes that regardless of control type (technical or procedural) the entity has the compliance requirement of implementing the control and demonstrating evidence of the control.

Question 2: Does the use of "technical controls" in Requirement R5.3 mean that each individual Cyber Asset within the Electronic Security Perimeter (ESP) has to automatically enforce each of the three R5.3 sub-requirements.

No, the IDT interprets the three sub-requirements within R5.3 no differently than the other sub-requirements of R5, with the exception of the technical feasibility exception (TFE) capability provided under R5.3. As requested under the request for interpretation, the concept of automatically enforcing controls is viewed by the IDT as the need to enforce the combination of the technical and procedural controls that are implemented to achieve strict compliance. The automatic enforcement component would apply to the technical controls that are implemented, however most procedural controls are not automatic. The IDT interprets that the responsible entity would need to demonstrate that controls have been put in place to achieve strict compliance with the three sub-requirements of R5.3. In the case where a specific device is not capable of implementing either a technical or procedural control, the entity would file for TFE treatment.