

Compliance Application Notice – 0017

CIP-007 R5 Technical and Procedural System Access and Password Controls

Posted: November 11, 2011

Primary Interest Groups

Compliance Enforcement Authority (CEA)¹

NERC

Regional Entity

Registered Entities subject to CIP Reliability Standards

Issue: Is a CEA to verify that technical controls, procedural controls, or both are implemented in assessing compliance with CIP-007² Requirement (R)5?

For the purpose of aiding a CEA, this CAN provides instruction for assessing whether a technical solution, a procedural solution or both are required for system access and password controls for a registered entity's Cyber Assets and Critical Cyber Assets to fulfill the requirements of CIP-007 R5.

- System Access Controls – R5, R5.1 and R5.2

First, this CAN provides instruction regarding when a CEA is to verify technical or procedural controls under R5.1 and R5.2, which state that a registered entity will establish, implement, and document technical *and* procedural controls, noting that both are not applicable to each of the actions contained in the sub-requirements of R5.1 and R5.2.

- Administrator, Shared, or Other Generic Account Passwords – R5.2.1

Second, this CAN clarifies that the passwords specified in R5.2.1 must comply with the password construction and change requirements contained in R5.3.

- Password Controls – R5.3

Third, this CAN provides instruction regarding when a CEA is to verify that a registered entity has a fully compliant technical solution.³

¹ Compliance Enforcement Authorities include ERO auditors, investigators, enforcement personnel or any person authorized to assess issues of concern, potential non-compliance, and possible, alleged or confirmed violations of NERC Reliability Standard requirements.

² The FERC order approving the Version 2 CIP Reliability Standards, CIP-002-2 through CIP-009-2, was issued in September 2009. See North American Electric Reliability Corp., 128 FERC ¶ 61,291 (September 2009 Order), order denying rehearing and granting clarification, 129 FERC ¶ 61,236 (2009). The FERC Order on Version 3 CIP Reliability Standards was issued on March 31, 2010. See North American Electric Reliability Corp., 130 FERC ¶ 61,271 (2010) (March 31 Order).

³ Registered entities' software, hardware and equipment have varying degrees of capability to provide a technical solution to fulfill the password control requirements of R5.3. Consequently, registered entities, under currently owned equipment, software, and security password schemes, may not have the ability to ensure compliance with the standard via a fully compliant technical solution.

- Technical Feasibility Exception (TFE)

Finally, this CAN provides instruction on when a CEA is to verify the entity has submitted a request for a TFE and whether the TFE request has been approved.

Summary of Compliance Application Notice

A CEA is to verify that a registered entity has implemented technical and procedural controls as required in the standards. In regard to R5.3, when an entity's Cyber Asset or Critical Cyber Asset is not capable of structuring passwords as required by the standard, then the CEA is instructed to verify whether the asset is covered under a TFE or the safe harbor of a TFE submission. In the case of a TFE submission, the CEA is instructed to verify whether the TFE-based compensating measures are in place. If a registered entity has submitted a TFE request, the entity will be subject to a safe harbor pending approval of the TFE, pursuant to section 5.3 of appendix 4D of the NERC Rules of Procedure.

Background

CIP-007 provides, in pertinent part:

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.*

R5.1. *The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.*

R5.1.1. *The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.*

R5.1.2. *The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.*

R5.1.3. *The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.*

R5.2. *The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.*

R5.2.1. *The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.*

R5.2.2. *The Responsible Entity shall identify those individuals with access to shared accounts.*

R5.2.3. *Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).*

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. [Emphasis added]*

Compliance Application

System Access Controls – R5, R5.1 and R5.2

NERC and the Regional Entities have determined that the “and” in R5 indicates that both technical and procedural controls are required throughout the sub-requirements R5.1 and R5.2, but both are not required for each of the actions required by R5.1 and R5.2. Therefore, a CEA is to verify that a registered entity has implemented the appropriate control(s) – either 1) both technical and procedural controls, or 2) only a procedural control – as required for each action. To clarify the first point, whenever a registered entity has a technical control, the technical control has been programmed to perform pursuant to a procedure, which is the procedural control. Therefore, whenever there is a technical control there is also an associated procedural control.

Examples:

R5.1.2 provides an example of a requirement where both procedural and technical controls are required. R5.2.1 requires an entity to establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails. Here, the methods, processes and procedures that generate the logs, to the extent they are electronic, would be a technical control. However, the entity also has a procedure that was programmed into the electronic solution that provides the procedural basis for the technical control and thus becomes the procedural control. A CEA is to verify the registered entity’s technical control is performing as intended.

R5.1.3 provides an example of a requirement where only a procedural control is required. R5.1.3 requires an annual review of user accounts to verify access privileges. Here, the annual review to verify access privileges may be a manual process, and, if so, would be conducted pursuant to a procedural control. Because the standard only addresses the review, there would be no technical control required by R5.1.3. Note that the procedural control is associated with

a technical database or software program (an employee is reviewing the electronically generated audit trails).

Administrator, Shared, or Other Generic Account Passwords – R5.2.1

A CEA is to verify that passwords that were changed prior to putting the system into service (as required by R5.2.1) meet the password construction and maintenance controls of R5.3, specifically password length (R5.3.1), password complexity (R5.3.2), and periodic password change (R5.3.2). The CEA should review the initial password controls as it does any other password controls per R5.3, as discussed below. If any of these password controls cannot technically be met (either initially or when changed), the CEA is to verify whether the registered entity has requested or obtained a TFE.

Password Controls – R5.3

A CEA is to verify that a registered entity requires and uses passwords, subject to the sub-requirements of CIP-007 R5.3. Where a registered entity owns equipment that has the capability – to whatever degree – to provide a technical solution, the CEA is to verify that the registered entity has the technical solution enabled, regardless if the technical solution has the ability to meet all of the requirements of the standard, as outlined below:

1. A technical solution is available:

If the software's technical solution fully meets the requirements of the standard, the CEA is to determine that the registered entity fulfills the requirement, and no further action is required.

Example:

A device supports at least six alphanumeric passwords (letters and numbers) and allows inclusion of special characters. If the device can be configured to require at least six characters in the password and can be configured to require letters, numbers and special characters, then there is a technical control and a procedural control, which would allow the registered entity to fulfill the requirements. For a CEA to find that the registered entity has met the requirements of R5.3.2 in this example, the CEA is to verify the registered entity implemented the technical control as specified in the procedural control.

2. A technical control is available but does not fulfill the requirements of the standard:

If a registered entity has equipment for which a technical control only partially meets the requirements of the standard, but the equipment has the capability to fulfill all requirements of the standard by also implementing a procedural control for the remaining requirements, the CEA is to verify that the registered entity has implemented a procedural control for any requirements that the technical solution cannot fulfill, and has obtained, or is in the process of obtaining, a TFE.

Example:

The server or workstation at issue runs a software application that 1) can configure a minimum password length, 2) can require complex passwords, and 3) will accept a fully compliant password. However, while the minimum password length of six characters can be enforced, setting the complex password option does not prevent a complex password from *not* including either a numeric digit or a special character. In other words, the requirements of R5.3.1 can be met, but the requirements of R5.3.2 cannot. For a CEA to find that the registered entity has met the requirements of both R5.3.1 and R5.3.2 in this example, the CEA is to verify that the registered entity had enabled the technical solution (set the minimum password length to at least six and enabled the complex password option), had further augmented the technical controls with a procedural control by implementing an internal policy and training program that requires numeric and special characters for passwords, and had submitted a TFE for the technical component.

Whether a procedural control is adequate is determined through the evaluation and approval of a TFE; however, a sufficient procedural control could include a procedural policy statement, personnel training, and other compensating measures, such as requiring longer passwords, restricting electronic access, and having a more frequent password change cycle.⁴

3. **Neither a technical control nor a procedural control can be implemented on the targeted Cyber Asset or Critical Cyber Asset device that will fulfill the requirements of the standard:** If a registered entity has a device that is incapable of fulfilling the password requirements of the standard through a technical solution, a procedural solution or a combination of both, the CEA is to verify that the registered entity has requested or obtained a TFE.

This situation may exist due to equipment restrictions for password lengths, equipment restricting the ability to change passwords, or password character sets not allowing the required diversity, among other reasons. The CEA is to verify that compensating technical or procedural controls are described in the TFE.

Example:

A piece of equipment can only support four numeric digits for a password. In this case, the device is not capable of configuring a compliant password at all. The registered entity can only rely upon procedural controls to require a four-digit password complexity; a six-character complex password is not possible. The CEA is not to find that the entity has met R5.3.2 in this example, and therefore is to verify that a TFE has been submitted.

⁴ CIP-007 R5.3.3 requires each password to be changed at least annually or more frequently based on risk.

Effective Period for CAN

This CAN is effective for CIP-007 upon posting as final on the NERC Web site, and is to be used by CEAs to assess compliance from the posting date forward, regardless of the start date of any non-compliance or Possible Violation. It supersedes all prior communications and will remain in effect until such time that a future version of a FERC or other applicable government authority approved standard or interpretation becomes effective and addresses the specific issue contained in this CAN.

For any enforcement action in process and for audits that have been initiated,⁵ a CEA will apply the appropriate discretion, including consideration of the specific facts and circumstances of the non-compliance, in determining whether to assess compliance pursuant to this CAN.

Evidence of Compliance

System Access Controls – R5, R5.1 and R5.2

A CEA is to verify that a registered entity implemented either 1) both a technical and a procedural control, or 2) only a procedural control, for each action required by R5.1 and R5.2 by reviewing:

1. documentation of the control(s) the registered entity has implemented for each required action; and
2. evidence that the control(s) fulfill the requirement of the specific action.

Administrator, Shared, or Other Generic Account Passwords – R5.2.1

A CEA is to verify evidence of the password change as described in the discussion of R5.3.

Password Controls – R5.3

1. **A technical solution is available:**

If the software's technical solution fully meets the requirements of the standard, a CEA is to review the registered entity's evidence demonstrating how its technical solution fulfills the requirements of R5.3.

2. **A technical control is available but does not fulfill the requirements of the standard:**

Where a registered entity's technical solution does not have the ability to fully meet the requirements of R5.3, a CEA is to verify that the registered entity 1) provided a procedural solution for any requirements that its technical solution cannot fulfill and 2) has obtained, or is in the process of obtaining, an approved TFE.⁶ Additionally, the CEA is instructed to review:

- a. the entity's approved TFE or submitted TFE request;
- b. evidence of the extent to which the entity's technical solution fulfills the requirement(s);
- c. documentation of the registered entity's procedural solution to meet the remaining requirements of R5.3;

⁵ "Initiated" means that a registered entity has received notification of the upcoming audit.

⁶ If a registered entity has submitted a TFE request, the entity will be subject to a safe harbor pending approval of the TFE, pursuant to section 5.3 of appendix 4D of the NERC Rules of Procedure.

- d. documentation of the registered entity’s training program to educate its affected personnel on its procedural solution as required by CIP-004; and
 - e. attestations from persons with overall responsibility for the procedural control (or alternative language: “attestations from persons responsible for implementing and/or overseeing compliance with the procedural solution”).
3. **Neither a technical solution nor a procedural solution can be implemented on the targeted Cyber Asset or Critical Cyber Asset device:**
- If the registered entity cannot implement a technical solution or a procedural solution on the Cyber Asset or Critical Cyber Asset, a CEA is to verify that the registered entity has obtained, or is in the process of obtaining, a TFE.⁷ Additionally, the CEA is instructed to review:
- a. the entity’s approved TFE or submitted TFE request, and
 - b. evidence of its implementation of the compensating measures (which may be on a different device) provided in its TFE.

For more information please contact:

Michael Moon
Director of Compliance Operations
michael.moon@nerc.net
404-446-2567

Valerie Agnew
Manager of Interface and Outreach
valerie.agnew@nerc.net
404-446-2566

This document is designed to convey compliance monitoring instruction to achieve a measure of consistency among auditors and Compliance Enforcement Authorities. It is not intended to establish new requirements under NERC’s Reliability Standards or to modify the requirements in any existing NERC Reliability Standard. Compliance will continue to be assessed based on language in the currently enforceable NERC Reliability Standards. This document is not intended to define the exclusive method an entity must use to comply with a particular standard or requirement, or foreclose a registered entity’s demonstration by alternative means that it has complied with the language and intent of the standard or requirement, taking into account the facts and circumstances of a particular registered entity. Implementation of information in this document is not a substitute for compliance with requirements in NERC’s Reliability Standards.

⁷ See footnote 6.