Project 2012-INT-04 Interpretation for ITC

Unofficial Comment Form

Project 2012-INT-04 Interpretation of CIP-007-3
Applicability Section and Requirement R5 for ITC

Please **DO NOT** use this form to submit comments. Please use the [electronic comment](https://www.nerc.net/nercsurvey/Survey.aspx?s=e065f290b55045d7857e4358daf9a235) form to submit comments on the Interpretation of CIP-007-3, Requirement R5, for ITC (Project 2012-INT-04). The electronic comment form must be completed by 8 p.m. ET **December 10, 2012.**

[Project Page](http://www.nerc.com/docs/standards/sar/ITC_Transmission_CIP-007-3_Request_for_an_Interpretation_to_NERC.pdf)

If you have questions please contact Steven Noess at steven.noess@nerc.net or by telephone at 404.446.9691.

### **Background Information**

In May 2011, the Standards Committee appointed a standing CIP Interpretation Drafting Team (IDT) for the development of CIP Interpretations. A project team from the CIP IDT has reviewed ITC’s request for interpretation and developed this interpretation pursuant to the NERC Guidelines for IDTs. (Available at: [Guidelines for Interpretation Drafting Teams](http://www.nerc.com/files/Guidelines_for_Interpretation_Drafting_Teams_Approved_April_2011.pdf)).

The stated purpose of CIP-007-3 is, in part, “to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).”

The IDT first examined the requests for interpretation (RFIs) from both TECO (Project 2012-INT-03) and ITC, and it determined that one interpretation effort could address both. In examining the two RFIs, the IDT identified the need to determine a commonly understood meaning of “procedural” and “technical” controls. The IDT used this meaning in its evaluation of the questions asked in the RFIs.

The IDT also recognized another area of work that is related to this topic introduced by NERC in CAN-0017. CAN-0017 determined that technical and procedural controls are required under R5.1 and R5.2, but both are not required for each sub-requirement. However, the CAN concluded that they were both required for the sub-requirements under R5.3 or the entity would need to demonstrate the existence of a TFE. The IDT reviewed this approach and believes that the interpretation of the language in the top level Requirement R5 would need to have a consistent application across all of its associated sub-requirements. The IDT notes that the current CIP-007-5 (as approved through recirculation ballot) has already addressed this applicability issue, and in specific conditions, it has applied technical or procedural control language. Further, if this interpretation receives industry approval, the IDT recommends that CAN-0017 be retired.

In examining the first question, the IDT performed an exercise to determine the scope of the language in the CIP-007 Requirement R5 top level requirement. In the exercise, the IDT examined each sub-requirement and evaluated the ability to apply both technical and procedural controls in each instance. In support of this exercise, the IDT developed a matrix of the R5 requirements, and it evaluated and discussed each for applicable controls. This matrix, with results and narrative, is supplied below as a reference to provide an understanding of the methodology used in this evaluation. The IDT determined that each requirement and sub requirement could not uniquely and independently be achieved by both technical and procedural controls. These findings led the IDT to a common understanding that CIP-007-3, Requirement R5 contains language that is to be achieved by an entity performing the collection of the activities contained within the sub-requirements. Therefore an entity would utilize a combination of technical and procedural controls in an effort to achieve strict compliance with the collection of requirements contained within Requirement R5, not specifically use both technical and procedural controls in achieving strict compliance for each unique sub-requirement. The CIP IDT acknowledges that the language within Requirement R5 would have been clearer had it read “technical *or* procedural controls”; however, changing the standard itself is outside the scope of the IDT. The IDT recommends that this language edit be included in further revisions of the standards.

In examining the second question of the RFI, the IDT examined the ability to automatically enforce controls placed on CIP-007-3, R5.3. Again, the IDT utilized the same process as in question 1, and it came to the same conclusion. In those requirements where an entity is utilizing a technical control, there could be an automatic enforcement capability of the technical control. In those conditions where a procedural control has been implemented, there would likely be no expectation of automatic enforcement. The word automatic is absent from the language within CIP-007-3, Requirement R5, and it is therefore not required to achieve strict compliance with the individual requirements or sub-requirements.

The IDT used the following table in developing this interpretation.

| **CIP-007-3****Requirement 5** | **Applicable Control** | **CIP IDT Evaluation** |
| --- | --- | --- |
| **Procedural** | **And/Or** | **Technical** |
| 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. | x | **And** | x | Technical and procedural controls shall be established, implemented, and documented to comply with Requirement R5 and the included sub-requirements. Any combination of technical controls or procedural controls may be applied collectively, provided there is at least one of each that would meet the requirement wording of using both technical and procedural controls. |
| 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. | x | **Procedural Controls Only/ or a combination of Procedural and Technical Controls** | **x** | The concept of "need to know" cannot be determined by an automated system. This must be determined by a Responsible Entity’s internal operational requirements. The appropriate access permissions must be documented in their procedures and reviewed against the configured access permissions. Ensuring user accounts are implemented with the appropriate access permissions could be performed by either a technical control (e.g. Identity and Access Management system) or a procedural control (e.g. manual review of the configured accounts). |
| 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. | x | **Or** | **x** | Ensuring user accounts are implemented as approved could be performed by either a technical control (e.g. Identity and Access Management system) or a procedural control (e.g. manual review of the configured accounts). |
| 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. | x | **Or** | x | A Cyber Asset must create logs with user account access activity. Without this technical ability it would be a violation of the requirement. In this instance a TFE is not permitted. For a technical control, a log file configured to retain logs for a minimum of 90 days and overwrite older records would be an example of a technical control. For a procedural control, alog file that stores 30 days worth of logs; the technical limit of the system, could be configured. Procedurally, the 30 day log files could be saved off of the Cyber Asset every 20 days. Saving five archives of the 20 day increments would meet the 90 day requirement. A technical control is not enforcing the 90 day in the second example. Alternatively, a procedural control could be implemented where a user logs into a Cyber Asset and manually logs their activity (e.g. in a protective relay under the single user account). |
| 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. | x | **Or** | **x** | The CIP IDT evaluated the applicable requirements CIP-003 R5 **(R5.2)** and CIP-004 R4 **(R4.1 and 4.2)**. Annually reviewing user accounts to verify access privileges could be performed by either a technical control (e.g.. Identity and Access Management system) or a procedural control (e.g.. manual review of the configured accounts). |
| 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. | x | **Or** | **x** | The Responsible Entity will define a policy for the acceptable use of the applicable account types. The policy could be implemented either via a technical control through an Identity and Access Management system or by a procedural control via the system admins only configuring the applicable accounts per the policy. |
| 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. | x | **Or** | **x** | The policy from 5.2 must contain the required provisions. The changing of passwords for administrator, shared, or generic accounts would require human interaction to identify the accounts and initiate the password change. Certainly, this would be accomplished through technical means; via a keyboard and mouse, but that is not the same as a "technical control." **There is a remote possibility that an Identity and Access Management system could be configured to perform this function but it is improbable.** |
| R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts. | x |   |   | One can use technical means to confirm the procedural component, but that is not the same as a "technical control." Identifying users with access to a shared account can be done by performing a "net group" dump of the users associated with a group. A paper list of the users that have been given access to the shared account for a protective relay could also meet the requirement. |
| 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). | x | **Procedural Controls Only/ or a combination of Procedural and Technical Controls** | **x** | A policy is required. Managing the use of shared accounts so that they can only be used by authorized personnel cannot be done by a technical control. A shared account can be used by anyone who has the user name and password, including those who are not authorized to do so. The CIP IDT does not know of an automated system to prevent this. Only a procedural control could be used for the use restriction. The audit trail of account use allows for the use of "automated or manual" means; therefore, either a technical or procedural control could meet that portion, as the requirement allows for either. The steps for securing accounts in the event of personnel changes could be performed via a technical control by an Identity and Access Management system or via a procedural control by a system admin changing the password on the Cyber Asset for the shared account. |
| R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible: | x | **Or** | **x** | A procedure could be used to require the use of passwords. A technical control would be to configure the Cyber Asset to always require the use of a password. |
| R5.3.1. Each password shall be a minimum of six characters. | x | **Or** | x | A procedure could be used to require passwords be a minimum of six characters. A technical control would be to configure the Cyber Asset to always require passwords be a minimum of six characters. |
| R5.3.2. Each password shall consist of a combination of alpha, numeric, and “special” characters. | x | **Or** | x | A procedure could be used to require passwords consist of a combination of alpha, numeric, and “special” characters. A technical control would be to configure the Cyber Asset to always require passwords 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. | x | **Or** | x | A procedure could be used to require passwords be changed at least annually. A technical control would be to configure the Cyber Asset to always require passwords be changed at least annually. |

**Questions:**

 **You do not have to answer all questions. Enter All Comments in Simple Text Format.**

*Insert a “check” mark in the appropriate boxes by double-clicking the gray areas.*

Please review the request for an interpretation, the associated standard, and the draft interpretation and then answer the following questions.

1. **Do you agree with this interpretation’s response to Question 1 (Whether each sub-requirement of Requirement R5 requires both “technical and procedural controls.”)? If not, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.**

[ ]  Yes

[ ]  No

Comments:

1. **Do you agree with this interpretation’s response to Question 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-parts.)? If not, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.**

[ ]  Yes

[ ]  No

Comments: