Project 2012-INT-04 Interpretation for ITC

**Unofficial Comment Form for Interpretation of CIP-007-3, Requirement R5, for ITC (Project 2012-INT-04)**

Please **DO NOT** use this form to submit comments. Please use the [electronic comment form](https://www.nerc.net/nercsurvey/Survey.aspx?s=d5997cbb86cb4f5188aaf65599ea6567) 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 **March 22, 2013**.

[Project page](http://www.nerc.com/filez/standards/2012-INT-04_Interpretation_CIP-007_ITC.html)

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 here](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, was supplied during an earlier posting, as part of the unofficial comment form, as background 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 satisfy 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.

Because the matrix was not all-inclusive, and because of concerns over future use of the matrix, the IDT has determined that, in the best interest of clarity and to promote focus on the interpretation itself, such a matrix should no longer accompany the background material. Therefore, the IDT has removed the matrix from the unofficial comment form.

**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: