Name (17 Responses)
Organization (17 Responses)
Group Name (14 Responses)
Lead Contact (14 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (1 Responses)
Comments (31 Responses)
Question 1 (29 Responses)
Question 1 Comments (30 Responses)
Question 2 (29 Responses)
Question 2 Comments (30 Responses)

Group
Northeast Power Coordinating Council
Guy Zito
Yes
No
The last sentence of the response needs clarification. Recommend changing from “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.” to “In the case where a specific device is not capable of implementing a technical control and it is not possible to implement a procedural control on that same specific device, the entity would file for TFE treatment.”
Individual
Thad Ness
American Electric Power
No
Though we agree with the overall interpretation provided to Q1, we disagree some of the insight provided. The interpretation appears to prescriptively require the use of technology within procedural controls when it states “the control is accomplished either by a human being using technology (procedural) or…”. Though we agree that technology may play a role in the procedural controls utilized, we disagree with any interpretation that actually requires using technology as part of that procedural control, as this is not specified within the standard itself.
No
Though we agree with the overall interpretation provided to Q2, we do not agree with the portion of the response that states “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”. It is not clear to us in what instance a device, by itself, could ever be considered a procedural control, as procedural controls typically occur outside of the inherent functionality of the device.
Individual
Nazra Gladu
Manitoba Hydro
Yes
Manitoba Hydro recommends removal of the following statement as it adds no value to the response: “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.” We acknowledge that the entity must show compliance to the controls deployed, as is the intention of any requirement.
Yes
Manitoba Hydro agrees the response to Question 2 in general, but doesn’t agree with the statement “The automatic enforcement component would apply to the technical controls that are implemented.

…" since it modifies the standard by adding an automatic enforcement requirement through the interpretation process, which is not allowed by the NERC Rules of Procedure. This statement should either be removed, or modified to "The automatic enforcement component could apply to the technical controls that are implemented, …" which does not make it a strict requirement.
Group
ACES COOP Members
Trey Cross
Yes
ACES, EKPC, AEPCO and SWTC appreciate the time and analysis from the IDT in determining that R5 requires a more flexible approach to compliance by allowing for an 'Or' when an 'And' is not possible. We would also like to add this language or similar for clarification; "In the case where a specific device is capable of implementing neither a technical or procedural control, the entity would file for TFE treatment."
No
If the IDT has determined that in to be compliant with R5.3, the entity can use technical and or procedural controls, R5.3 and the sub-parts should be able to have procedural controls; if technically not possible. Thank you for the time and consideration.
Individual
Cade James Simmons
MidAmerican Energy Company
Yes
Yes
Group
Southern Company
Shane Eaker
Yes
Yes
Southern Company reads the IDT's response to Question 2 to state that, with respect to the context of R5.3, either technical or procedural controls may be used to demonstrate strict compliance with subrequirement R5.3 or one of its sub-subrequirements, so long as some combination of technical and procedural controls are used to demonstrate compliance with Requirement 5 and its various subparts as a whole. In its last sentence, the IDT states that, "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." To clarify and remove all doubt as to the reading of this phrase, Southern would suggest phrasing the last sentence in the following manner: "In the case where neither a technical nor a procedural control is capable of implementation for a specific device, the entity would file for TFE treatment with respect to R5.3 and its various subparts.
Group
Hydro One Networks Inc.
Sasa Maljukan
Yes
Yes
To improve clarity, we recommend changing last sentence from " 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. " to " In the case where a specific device is not capable of implementing a technical control

and it is not possible to implement a procedural control on that same specific device, the entity would file for TFE treatment." Also, Hydro One believes that this interpretation clarifies the issue discussed in the CAN-0017 document. Because of this we suggest NERC considers retiring it.
Group
Bonneville Power Administration
Chris Higgins
Yes
Bonneville Power Administration (BPA) notes that the interpretation does not give an explicit answer to Question 1. BPA strongly agrees with the statement "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.", and notes the following issues: First, the matrix of R5 requirements is not part of the interpretation, and should not be held as directive on Responsible Entities. BPA suggests that the sentence in the fifth paragraph of the Background ending "…understanding of the methodology used in this evaluation." be revised to "…understanding of the methodology used in this evaluation, but is not directive on the Responsible Entities." Second, the evaluation of R5.1.2 in the matrix states "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." This appears to clearly deny the use of procedural controls. However, the last sentence in the evaluation of R5.1.2 explicitly allows procedural controls. BPA believes that there is no requirement that the Cyber Asset itself create logs, especially since the requirement is to produce "methods, processes, and procedures" without referring to technical controls. Finally, the evaluation of R5.3 in the matrix states "A procedure could be used to require the use of passwords." This implies that the intent of R5.3 is that all systems must use passwords, and the passwords must meet the subrequirements. It is equally valid to take R5.3 as describing the requirements that passwords must meet if passwords are used. BPA believes that the latter is the correct meaning, for several reasons. One, authentication methods such as two-factor authentication, which is much stronger than the use of passwords, would not be compliant under the first interpretation. Two, a system which allows only weak passwords might be better protected by other means such as physical access control. Three, there are legacy systems which do not have the capability to use passwords, but for which other access control methods such as physical access control can enforce adequate security.
Yes
BPA notes that the Interpretation does not give an explicit answer to Question 2. BPA strongly agrees with the statement "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.", as long as "it" refers to the use of automatic enforcement of the requirements. Also, see comments about the matrix of R5 requirements in the comments for Question 1.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
Yes
Group
ISO/RTO Council Security Working Group
Greg Goodrich
Yes
No
The ISO/RTO Council Security Working Group does not agree with the response's because the last

sentence is not clear enough. The ISO/RTO SWG recommends changing from "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." to "In the case where a specific device is not capable of implementing a technical control and it is not possible to implement a procedural control on that same specific device, the entity would file for TFE treatment."
Individual
Patrick Brown
Essential Power, LLC
Yes
Yes
Individual
Don Jones
Texas Reliability Entity
No
Texas RE finds the proposed Response to Question 1 to be unduly long and complicated. The answer should simply be “In R5, the reference to ‘technical and procedural controls’ means both technical controls and procedural controls or either one of them, as appropriate in each context.” This interpretation is consistent with common and acceptable usage of the word “and” in written materials. (For the engineers, this usage corresponds to the logical OR function.)
No
The proposed response answers only part of Question 2. (1) Texas RE agrees that R5.3 does not have to be enforced “automatically,” if that means by using only technical controls. The sub-parts of R5.3 may be enforced by procedural controls as well as by technical controls. (2) The response should make clear that ALL of the sub-parts of R5.3 are required, as technically (or procedurally)feasible. (3) Texas RE would prefer not to invite additional TFE filings in this context. If one of the sub-parts of R5.3 is not technically feasible as applied to a specific Cyber Asset, the registered entity should be prepared to demonstrate either compliance or infeasibility at the time of an audit or spot check.
Individual
Randi Nyholm
Minnesota Power
Yes
Yes
Group
Dominion
Connie Lowe
Yes
No
In general, Dominion agrees with the response; however, the last sentence could still be misinterpreted as requiring a TFE to be filed if only one type of control is available (technical or procedural). Dominion suggests the last sentence of the response be rewritten as follows, “A TFE should be filed if neither a technical control nor a procedural control can be implemented for requirement 5.3 or any of its individual sub-requirements for a specific device.”
Group
Associated Electric Cooperative, Inc. - JRO00088

David Dockery
Yes
AECI supports this determination and the underlying rationale.
Yes
AECI supports this determination and the underlying rationale
Group
FirstEnergy Corp
Larry Raczkowski
Yes
FirstEnergy agrees it should not be necessary to implement both technical and procedural controls to comply with the sub-requirements of CIP-007 R5. We agree with the IDT view that since CAN-017 contradicts this position, it is important that CAN-0017 is retired if/when this interpretation becomes effective.
Yes
FirstEnergy agrees that procedural controls provide an acceptable means to enforce all three sub-requirements of CIP-007 R5; technical controls should not be required. More importantly, registered entities should not be required to generate and maintain Technical Feasibility Exceptions (TFEs) when procedure controls are implemented as the sole means of enforcing these sub-requirements. Very few cyber assets provide technical controls to enforce all three sub-requirements; consequently, registered entities are currently required to generate and maintain TFEs for virtually all of their CIP cyber assets. Since these TFEs normally just document the alternate procedural controls used to enforce these requirements, these TFEs represent a tremendous administrative burden with no improvement in BES reliability.
Group
Duke Energy
Greg Rowland
Yes
Duke Energy agrees with the response to Question 1.
Yes
Duke Energy agrees with the response to Question 2.
Individual
Shari Heino
Brazos Electric Power Cooperative, Inc.
ACES Power Marketing
Yes
No
The language is not clear. This sentence from the response to question 2 is vague because of the use of “either”: “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.” Consider rewriting it as: “In the case where a specific device is capable of implementing neither a technical nor procedural control, the entity would file for TFE treatment.”
Group
Entergy
James Gower
Yes
Entergy agrees with this interpretation of the requirements that both technical and procedural controls could be used to enforce access authentication. Where technical controls can not be implemented procedural controls will be established and implemented which require technical actions.

Additionall, the latest draft of CIP version 5, states the following in regards to passwords: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non alphanumeric) or the maximum complexity supported by the Cyber Asset. The intent of the CIP v5 draft requirements acknowledges the limited risk to the BES by not requiring both technical and procedural controls which is consistent with Entergy's current interpretation. Entergy realizes that CAN-0017 released by NERC on November 11, 2011 is contrary to our interpretation of the requirements, however per a NERC presentation delivered on March 30, 2011, the "Purpose of CAN does not modify a reliability standard and is not a replacement for an interpretation". Currently, there is no formal NERC interpretation for this requirement.
Yes
Individual
Bill Fowler
City of Tallahassee
Yes
Yes
Individual
Michael R. Lombardi
Northeast Utilities
Yes
NU supports this interpretation and also recommends that CAN-0017 be retired.
Yes
NU supports this interpretation and also recommends that CAN-0017 be retired.
Individual
Brett Holland
Kansas City Power & Light
Yes
Yes
Individual
Patricia Boody
Tampa Electric Company
Yes
Tampa Electric complements the IDT for their work in drafting this Response to the Interpretation for ITC. Tampa Electric agrees with the response to Question 1. In addition, we recommend that the IDT consider a way to include the table from the Unofficial Comments document as it provides additional clarity and information for compliance/audits. In addition, this RFI is similar to Interpretation 2012-INT-03 submitted by TECO. We recommend that the IDT address both Interpretations with the upcoming ballot. Tampa Electric requests the IDT/NERC to provide guidance to Registered Entities/Regional Entities related to TFEs that will no longer be required so that there is a uniform process across all regions. Our current options include (1) termination by the Registered Entity (2) the disapproval of a TFE by the Regional Entity. Tampa Electric recommends a termination of the TFE by the effective date of the approved RFI.

Yes
Individual
Anthony Jablonski
ReliabiltiyFirst
No
ReliabilityFirst generally agrees with the drafted question 1, CIP-007 Interpretation, but offers the following comments for consideration: The IDT does a good job of discussing the differences between technical and procedural controls, but the discussion becomes unclear when discussing the requirement for implementing each type of control. Also, the wording of the actual Interpretation is at odds with CAN-0017. CAN-0017 states "…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", meaning that procedural controls are necessary for all requirements and sub-requirements, and may be supported by technical controls as appropriate. ReliabilityFirst agrees with CAN-0017 that technical controls that support procedural controls work. ReliabilityFirst does not agree that a technical control without an associated procedural control will be an effective method of implementing compliance with a requirement. ReliabilityFirst recommends the wording of the Interpretation be changed and clarified to ensure procedural controls are required for all requirements and sub-requirements to be consistent with CAN-0017.
No
ReliabilityFirst generally agrees with the drafted question 2 CIP-007 Interpretation, but offers the following comments for consideration: The IDT's language changes the reading of CIP-007-3 R5.3 to somewhat correspond with the wording contained in CIP-007-5 R5 Parts 5.5 and 5.6. This may ease the entities' transition into CIP Version 5 without seriously compromising security of existing systems. However, the Interpretation needs to be clarified to ensure that technical controls for password length, complexity and age are implemented when they are available. This in enforced now by the practice of denying a TFE in the case where compliance with a requirement is "technically feasible." If a technical control is available but not used, compliance will revert to reliance on a (presumably weaker) procedural control, which will increase risk to the BES. ReliabilityFirst recommends that the wording of the answer to Question 2 be modified to ensure that a technical control is implemented if it is available for a particular Cyber Asset.
Group
PPL NERC Registered Affiliates
Brent Ingebrigtson
We agree with the interpretation, however, in support of this we believe that CAN-0017 should be revisited to address the language requiring a TFE for purely procedural controls. Specifically, number 2 in the Section "Password Controls – R5.3", currently it reads: "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 the standard by 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 a technical solution cannot fulfill, and has obtained, or is in the process of obtaining, a TFE." With this interpretation we believe it should be rewritten to delete the part requiring a TFE, "…the CEA is to verify that a registered entity has implemented a procedural control for any requirements that a technical solution cannot fulfill."
Individual
Andrew Gallo
City of Austin dba Austin Energy
Agree
Electric Reliability Council of Texas, Inc. ("ERCOT").
Individual
Michael Moltane
ITC

Yes
Yes
ITC supports the results of the RFI, Interpretation 2012-ITC-04 – Interpretation of CIP-007 for ITC. However, due to long delay in this Interpretation process (~18 months since we submitted our Request for Interpretation), we have planned around this by filing a large number of Technical Feasibility Exceptions denoting compensating/mitigating measures. We encourage NERC and the industry to continue work on development of a faster response time for Interpretation Requests to make them more useful in the future. ITC would also like to point out that since some portions of this Interpretation are in conflict with CAN-0017, that the CAN should be retired.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
While the SPP RE agrees with the response language specific to Question 1, the SPP RE has concerns with the interpretation documentation overall. The analysis matrix should be included in the formal interpretation in some manner, subject to the following comments: The analysis matrix discussion for R5.1.2 contains what appears to be misleading guidance. After a good discussion of the need for an automated (technical) logging capability, possibly augmented with a procedural log retention control, the discussion makes reference to manually logging access to a relay via a single account. This final observation is not appropriate for R5.1.2 as the use of a single access credential by multiple relay technicians is a shared account subject to the requirements of R5.2.3. As readers of the interpretation may rely upon the analysis discussion, this aspect of the analysis needs to be corrected. Additionally, the bolded comment for R5.2.1 may need to be changed or removed. There are commercial applications available, such as Cyber Ark, that will manage shared and administratively privileged accounts by automatically changing the passwords per an entity policy, secure those passwords in an access controlled vault, and log by individual user and date/time of access who has obtained the password for a specific system and user account. The characterization that such a capability is improbable is likely not warranted. This comment is also applicable to R5.2.3 where the discussion states that managing the use of a shared account cannot be performed by a technical control. To the contrary, utilities such as Cyber Ark are designed to do exactly that. The key is to configure the password change policy to establish a one-time-use password for each access and to control authorization via the authentication rights to the password management system and vault.
No
The interpretation asserts that the mere presence of a procedural control is sufficient to demonstrate compliance with R5.3 and its included requirements. While the standard does not prescribe the use of technical controls to assure and enforce strict compliance, the absence of such controls means that strict compliance cannot be assured. In the absence of a technical control whose configuration can be evaluated at audit, the registered entity is not able to demonstrate strict compliance short of disclosing the passwords to the auditors, something the audit teams are not willing to pursue. In effect, in the absence of auditable technical controls, this requirement is essentially not auditable and the entity cannot demonstrate compliance. Therefore, in the absence of technical controls that can be configured to enforce strict compliance, the registered entity's only recourse is to seek a Technical Feasibility Exception to provide safe harbor from a violation and apply procedural controls as the compensating and mitigating measures required by the TFE. The recommendation to retire CAN-0017 with the adoption of this interpretation is premature.
Individual
Cheryl Moseley
Electric Reliability Council of Texas, Inc.
Yes
No
We do not agree with this response because the response's last sentence is not clear enough. We

recommend changing from " 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. " to " In the case where a specific device is not capable of implementing a technical control and it is not possible to implement a procedural control on that same specific device, the entity would file for TFE treatment." ERCOT Recommendation: Recommended change to the last sentence: “In the case where a technical and/or procedural control cannot be implemented or supported for a specific device, the responsible entity is advised to request a TFE in accordance with Appendix 4D of the NERC Rules of Procedure.”
Individual
David Jendras
Ameren
No
(1)Ameren agrees in part with the IDT interpretation; specifically we agree with the need for clarification of the suggested language change to read “technical or procedural controls”. (2)We request clarification to expound on what is expected to be compliant with this requirement. Is the intent of the language change to provide situational guidance or is it to be applied literally? In other words, will the requirement now require either a technical control or a procedural control under any circumstance, or is the requirement requiring a technical control wherever possible and procedural control when it is not feasible to use technical controls? Without clarification in the requirement language as to how and when to apply the requirement, there will be a continued opportunity for misinterpretation. (3)The interpretation should clearly indicate whether or not when a technical control is feasible it should be used and if it is not technically feasible, then a procedural control is acceptable and finally it should clarify when a TFE will be required.
No
(1)We believe there may be a conflict between the responses for the two interpretation questions on how the requirement R5.3 should be interpreted and further clarification is requested. (a)First; the word “automatic” is not being considered as directive and is not required to achieve strict compliance and there is no mention of using the TFE process to support non-compliance. (b)Second; in reference to “technical controls”, the word “automatic” is being treated as being directive and is required to achieve strict compliance with sub-requirements of R5.3. (2)We believe that the IDT response does not clearly indicate whether or not all Cyber Assets within an ESP must comply with the R5.3 requirements or if only the CCAs need to comply. We believe this requirement applies to all Cyber Assets with the ESP and where neither a procedural or technical control is feasible then it requires the filing of a TFE.
Group
Salt River Project
Bob Steiger
Yes
Yes