Individual or group. (18 Responses)
Name (13 Responses)
Organization (13 Responses)
Group Name (5 Responses)
Lead Contact (5 Responses)
Contact Organization (5 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (2 Responses)
Comments (18 Responses)
Question 1 (15 Responses)
Question 1 Comments (16 Responses)
Question 2 (15 Responses)
Question 2 Comments (16 Responses)

Group
Northeast Power Coordinating Council
Guy Zito
Northeast Power Coordinating Council
Yes
Yes
Individual
Shannon Fair
Colorado Springs Utilities
Yes
Colorado Springs Utilities agrees with the interpretation INT-04 CIP-007-3, but it appears to be in conflict with CAN0017.
Yes
Group
MISO
Dave Francis
MISO
Agree
MISO, SPP, PJM
Group
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing
Pamela Hunter
Southern Company Operations Compliance
Yes
Yes
Group

Dominion NERC Compliance Policy
Randi Heise
Dominion
Yes
Yes
Individual
Nazra Gladu
Manitoba Hydro
No comment.
No comment.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Agree
ATC endorses the comments submitted by MRO NSRF.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Southwest Power Pool Regional Entity
Yes
Yes
While the interpretation response to Question 2 is technically correct, SPP RE remains concerned that entities would be ill advised if they do not seek a Technical Feasibility Exception for those instances where technical controls cannot enforce the technical password configuration requirement of the standard. Many, but not all operating systems readily support the setting of a configuration control prescribing a minimum password length and a maximum password age. Most operating systems do not have the capability to prescribe a password complexity that fully meets the CIP-007-3/R5.3.2 requirement. At audit, registered entities are obligated to demonstrate compliance with the requirement. Having a procedural control, such as a password policy, instructs the user to conform but does not demonstrate that the user has actually conformed to the requirement. Compliance can be demonstrated by disclosing the password to the auditor, but that is something neither the entity nor the auditor is willing to do for cyber security reasons. That places the registered entity in a dilemma. Unless conformance can be demonstrated, compliance cannot be demonstrated and the registered entity is at risk of a possible violation. Procedural controls, along with configuring the operating system to enforce password complexity to the maximum extent possible, are good mitigating measures to support a Technical Feasibility Exception. Appendix 4D of the NERC Rules of Procedure provides for and requires a TFE for any instance where the entity cannot comply with CIP-007-3, Requirement R5 or one or more of the included requirements R5.3.1, R5.3.2, and R5.3.3. The TFE is also available and appropriate when the registered entity cannot demonstrate compliance, regardless whether actual compliance can be achieved, for the express purpose of safe harbor from a violation. The SPP RE strongly recommends the interpretation be modified to at least recommend the pursuit of a TFE in those instances where technical enforcement of the requirement is not possible. The registered entity can then make an informed decision whether to seek a TFE or risk a possible violation at audit.
Individual
Michael Falvo

Independent Electricity System Operator
Yes
Yes
Individual
John Seelke
Public Service Enterprise Group
Yes
We support the interpretation language and have a minor request for clarification. The interpretation as is written allows either a technical and/or a procedural control to comply with the sub-requirements R5.3.x on an individual basis. Recognizing that where technically possible a device should enforce the password characteristics, does the interpretation remove the ability for an entity to submit a TFE for these sub-requirements if they are using only a procedural control? (i.e. can an entity file a TFE on password complexity and use a procedural control as one of the mitigation actions for such a TFE, or is the intent to no longer have such TFEs submitted?)
Yes
Individual
Wryan J. Feil
Northeast Utilities
Yes
To meet this requirement, procedural controls should be sufficient since enforcement and training permeate through many other CIP requirements where procedural controls are sufficient.
Yes
However, the last sentence of the IDT interpretation needs strengthening. See the following: "The IDT interprets that the responsible entity would need to demonstrate that the [Insert word: procedural] controls have been put in place to satisfy the three sub-requirements of R5.3.
Individual
Anthony Jablonski
ReliabilityFirst
No
The IDT correctly states, “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.” However, there is no basis in the language of the requirement for the following statement, “Both are not necessary for each sub-requirement individually.” Had the language of the requirement read “technical or procedural controls,” then the IDT would have a firm basis for this statement. The result of the IDT’s Interpretation is to effectively change the language of the standard.
No
The IDT extends the unjustified reading of Requirement R5 in Question 1 into the sub-requirements of Requirement R5.3. As in Question 1, there is no basis in the language of the Requirement for this reading.
Individual
RoLynda Shumpert
South Carolina Electric and Gas

Yes
The interpretations says "...it is not necessary for both technical and procedural controls to be used in each subrequirement of Requirement R5." and I agree that it should be one or the other but not necessarily both as the word "and" implied.
Yes
Individual
Brian S. Millard
Tennessee Valley Authority
Yes
Yes
TVA would like the IDT to clarify if a TFE is needed where there is a procedural control in place in the event technical enforcement is not possible. With the IDT's clarification to Question 1 that both technical and procedural controls are not necessary for each sub requirement, the argument could be made that a TFE not required when using a procedural control.
Individual
Warren Cross
ACES
Yes
ACES supports the interpretation of moving from a "technical and procedural controls" to a "technical or procedural controls" understanding.
Yes
ACES supports the understanding that automatically enforcing controls is the combination of the technical and procedural controls that are implemented to satisfy the three sub-requirements of R5.3.
Individual
Thad Ness
American Electric Power
Yes
Yes
Individual
Russel Mountjoy
Midwest Reliability Organization
No
MRO does not support the interpretation of CIP-007-3 for ITC as presented. CIP-007-3 R5 clearly states the Responsible Entity shall establish, implement and document technical "and" procedural controls….the requirement does not offer the choice of technical "or" procedural controls, the requirement requires both through the use of "and".
No
Technical controls providing reminders for registered entities to change passwords are necessary; however, the technical controls should not be automatically changing the passwords themselves
Individual
Brett Holland
Kansas City Power & Light

Yes
No
It would be helpful to add additional clarification regarding the TFE requirements for CIP-007-3 R5.3. A statement should be added that indicates it is possible to implement procedural controls without also requiring a TFE. There may be instances where the three R5.3 sub-parts are not automatically enforced, though procedural mechanisms are used to ensure that technically feasible password configurations or periodic activities are met.