

CAN-0017 Comment Analysis Summary

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

CAN-0017 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. The draft CAN was posted for industry comment on the NERC web site on September 23, 2011 and the comment period expired on October 14, 2011.

NERC received approximately 23 comments from various industry stakeholders and trade associations, which are identified below. The main themes of the comments consisted of the following four categories: errata changes, scope, effective date and evidence of compliance.

Errata

Errata changes were made in order to correct a few typos and to change the number of a footnote.

Scope

There two industry groups that recommended substantive changes to the CAN in regard to scope. There were several comments that stated a procedural control is permitted by the standards and a TFE should not be required. It is understood that the compliance application may generate additional TFE's when the TFE is process is already overburdened, however, after legal review, it was determined that the compliance application stated in the CAN is required by FERC Orders.¹

R5 specifies the need for technical and procedural controls. R5.1 does not use the words "where technically feasible"² and thus a TFE is not required where a procedural solution is the appropriate solution. R5.2 also does not use the words "where technically feasible" so again, a TFE is not required nor available. In the case of R5.2.1, the CAN provides for the availability of a TFE as the passwords must be changed in accordance with R5.3. R5.3 requires and provides for the availability of a TFE.

Additionally, a comment was made in regards to the CEA verifying the adequacy of the controls submitted in the TFE, specifically that this is not the role of the CEA. The CAN was modified to remove the instruction that CEAs are to verify the adequacy of compensating measures.

¹ See 133 FERC ¶161,008, Order on Compliance Filing Docket No. RR10-1-001 (October 1, 2020) and NERC Rules of Procedure Appendix 4D.

² *Id.*

Effective Date

Several commenters believe that NERC should to incorporate a reasonable implementation period for CAN-0017 to allow for time to file a Technical Feasibility Exception (TFE) with the applicable Regional Entity.

In response, CAN-0017 is effective for CIP-007 R5 upon posting as final on the NERC Web site. Registered entities should be aware that auditors will be using the guidance in CAN-0017 for assessing compliance from the posted date going forward, however a submitted TFE will provide a safe harbor until the TFE is approved. Additionally, CEAs will use discretion in whether the CAN is to be applied to any entity who has received notification of an upcoming audit.

Evidence

Commenters had questions regarding the Evidence of Compliance section. Particularly, several industry members stated that the standard did not reference training and there is not an obligation to provide training under CIP-007 R5.

In response, the evidence listed in the CAN includes several options that CEA staff can look for to verify compliance with the standard. One of the key concerns was CEAs verifying evidence of training. Although CEAs are not to verify adequacy of compensating measures as compensating measures are to be evaluated through the TFE process, a CEA does need to verify that the compensating measures have been implemented. Training is one way to ensure that an entity's staff is aware of the procedural control. Training may be conducted in a variety of methods and evidence of such training may include interviews with the applicable personnel. Additionally, the Evidence of Compliance section states, "may include but is not limited to," to account for the fact that entities may or may not have a specific type of evidence.

Conclusion

The analysis spreadsheet for CAN-0017 is also posted on the NERC website. While the spreadsheet format did not provide sufficient information to provide industry with visibility into the effort that is put into reviewing all of the comments, it is hoped that this document will supplement that information. Feedback from all sources is key and NERC staff thanks industry for the time and effort put into providing that feedback. If you would like further discussion on CAN-0017, please feel free to contact us at cancomments@nerc.net.

Registered Entities that submitted CAN Comments

ACES Power Marketing

Ameren Services

American Electric Power (AEP)

Arizona Public Service (AZPS)

Bonneville Power Administration (BPA)
Constellation Energy (CEG)
Dominion Resources Services, Inc.
Epoch Technical Solutions
ITC Holdings
Kansas City Power & Light (KCP&L)
LG&E and KU Energy
Madison Gas and Electric (MGE)
MidAmerican Energy Company
PacifiCorp
Pepco Holdings, Inc.
PGN
PPL Electric Utilities
Southern Company
Westar Energy
Xcel Energy

Trade Associations that submitted CAN Comments

Edison Electric Institute (EEI)
National Rural Electric Cooperative Association (NRECA)
ISO/RTO Council Standards Review Committee (IRC SRC)