

CAN-0007 Comment Analysis Summary

CIP-004 R2.4 Revocation of Access to Critical Cyber Assets

CAN-0007 was originally posted as final on December 2, 2010. The original CAN provided instruction for assessing whether registered entities revoked access to CCAs as required in CIP-004 R4.2. CAN-0007 also outlines acceptable scenarios for using a technical feasibility exception (TFE).

The revised CAN was reposted as final on December 9, 2011, and it incorporates the direction provided by the NERC Board of Trustees in August of 2011.

The draft of the revised CAN was posted for industry comment on the NERC web site on September 1, 2011, and the comment period expired on September 21, 2011. NERC received 12 comments from registered entities and 4 comments from industry trade associations, which are identified below. The main themes of the comments consisted of the following three categories: errata changes, the scope of the CAN and the effective date.

Errata

Many recommended errata changes were to update the Primary Interest Groups section to be consistent with the applicability section of CIP-004. After further review, the applicable functional entities were added to the Primary Interest Groups section. The exemptions to applicability provided in the standard and are not repeated in the CAN.

Another comment stated that there were repetitive statements about clarification on access and clarification on electronic access. In response to this comment, the repeated paragraphs were removed.

Scope

There were several recommended substantive changes to the CAN in regard to the scope of the compliance guidance.

The commenters stated that CAN-0007 appears to expand the requirement and many of the draft CAN details are outside the context of what is intended by the initial issue. In response to the comments, the issue question was clarified to state, "What evidence does a CEA seek to determine whether entities revoked access to Critical Cyber Assets (CCAs) as required in CIP-004 R4.2?"

The CAN was revised to state that a CEA is to verify that an individual whose access has been revoked is not able to access the CCA.

For entities that have multiple levels of control (commonly referred to as “defense in depth”), this does not mean that all revocations comprising the “defense in depth” strategy must be complete within the specified time frames, but sufficient revocations to deny that entity access to the CCA must be complete within the specified time frames in the standard.

The CAN provides instruction that a CEA is to use discretion with regard to the type of evidence verified for revocation of access. The evidence will vary depending upon the entity and the specific circumstances surrounding the revocation.

Effective Date

Several commenters believe that NERC should incorporate a reasonable implementation period for all CANs. Other commenters suggested that a CAN should become effective only after it is publicly posted by NERC as final and provides an effective date that cannot be earlier than the posted date. There has been confusion from the industry about the date stated in the Effective Period of CAN section, as it refers to the date of the previously posted version.

The effective date of CAN-0007, which is the date CEAs are to begin using the compliance application to assess compliance, is December 9, 2011, the date this version of the CAN is posted as final on the NERC Web site. It is to be used by CEAs to assess compliance from the posting date forward, regardless of the start date of any non-compliance or Possible Violation.

For any enforcement action in process and for audits that have been initiated,¹ a CEA is to apply the appropriate discretion, including consideration of the specific facts and circumstances of the non-compliance, in determining whether to assess compliance pursuant to this CAN.

Conclusion

The analysis spreadsheet for CAN-0007 is posted on the NERC website. The spreadsheet format did not provide sufficient information to offer industry visibility into the effort that is put into reviewing all of the comments, and it is hoped that this summary analysis 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-0007, 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)

¹ “Initiated” means that a registered entity has received notification of the upcoming audit.

Bonneville Power Administration (BPA)
Consumers Energy
Dominion Resources Services, Inc.
Exelon Corp.
Farmington Electric Utility
Kansas City Power & Light (KCP&L)
MidAmerican Energy Company
Southern Company
Xcel Energy

Trade Associations that submitted CAN Comments

Edison Electric Institute (EEI)
ISO/RTO Council's Standard Review Committee (IRC SRC)
Midwest Reliability Organization NERC Standards Review Forum (MRO NSRF)
National Rural Electric Cooperative Association (NRECA)
NPCC Entities (Industry)