

CAN-0005 Comment Analysis Summary

CIP-002 R3 Critical Cyber Asset Designation for System Operator Laptops

CAN-0005 was originally posted as final on July 6, 2010 and has undergone several revisions since the original posting, the last of which was on March 24, 2011. The original CAN provided guidance regarding whether system operator laptops with the capability and purpose of controlling Bulk Electric System assets remotely (whether in normal operations or in emergencies) should be designated as Critical Cyber Assets (CCAs). The CAN was revised to incorporate the direction provided by the NERC Board of Trustees in August of 2011, and a material change was made to the compliance application section. The CAN was reposted as final on December 9, 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 16 comments from registered entities and four comments from industry trade associations, which are identified below. The main themes of the comments consist of the following five categories: errata changes, the scope of the CAN, the effective date language and the types of evidence CEAs are to verify.

Errata

The recommended errata changes were made in order to remove an incorrect reference to the SDT Project 2008-06 Cyber Security 706.

Scope

There were substantive changes made to the CAN in regard to the scope of the compliance guidance. Commenters stated that CAN-0005 appears to expand the requirement and that many of the draft CAN details are outside the context of what is intended by the initial issue.

NERC received a suggestion to revising the CAN to only provide what is an acceptable audit approach to verify that registered entities designated system operator laptops as Critical Cyber Assets (CCAs) based upon the registered entity's procedures. In response, NERC staff changed the CAN to state that the registered entity is to determine which assets are designated as Critical Assets and associated Critical Cyber Assets. It is impractical for a CAN to attempt to identify applicability, given the multitude of situations in which various laptops may have the "capability and purpose to control critical assets," and therefore, it was concluded that the registered entity is in the best position to make the determination of which laptops are used as a CCA.

Other commenters stated that there were other situations that would also apply to this situation, such as remote desktop computers. In response, the material revision applies broadly and addresses this concern. CAN-0005 was revised to state, "CEAs are to verify that registered entities followed their own

internal back-up, emergency and evacuation procedures to properly identify Cyber Assets that are essential to the reliable operation of Critical Assets as Critical Cyber Assets, including normal, back-up and emergency operations. This may or may not include identification of system operator laptops or other remote access technology as Critical Cyber Assets.”

Further, the CAN was revised based on comments that the current version of CAN-0005 would reduce to the efficiency of emergency preparedness and would limit the use of laptops. In response, the revised version of the CAN states that, “the registered entity is in the best position to make the determination of which laptops are used as a CCA.”

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-0005, which is the date CEAs are to begin using the compliance application to assess compliance, is 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.

Additionally, this version supersedes all prior communications and prior versions of CAN-0005. ***For any enforcement action in process*** and for audits that have been initiated,¹ a CEA will 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.

Evidence

The evidence of compliance section in the CAN was revised to provide instruction to CEAs when assessing compliance with CIP-002 R3. The revised evidence section stated that CEAs are to verify the registered entity’s list of Critical Cyber Assets and the process for identifying these Critical Cyber Assets. Please note that CAN-0005’s reference to a process is not meant to add another requirement to the standard, but rather to provide instruction to CEAs to verify types of documentation.

If a registered entity has a documented identification process, CEAs are to verify that document and determine if system operator laptops were considered. If there is not a documented process, CEAs are to interview the registered entity’s personnel and verify other supporting evidence. The CEA is to

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

verify that the registered entity's list of Critical Cyber Assets is complete pursuant to the registered entity's identification process.

Conclusion

The analysis spreadsheet for CAN-0005 is posted on the NERC website. Since the spreadsheet format did not provide sufficient information to industry with regard to the effort that NERC puts into reviewing all of the comments, 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-0005, please feel free to contact us at cancomments@nerc.net.

Registered Entities that submitted CAN Comments

ACES Power Marketing
American Electric Power (AEP)
Austin Energy
Bonneville Power Administration (BPA)
Central Lincoln
Consumers Energy
Constellation Energy (CEG)
Dominion Resources Services, Inc.
Farmington Electric Utility
Florida Municipal Power Authority (FMPA)
Fort Pierce Utilities Authority (FPUA)
Kansas City Power & Light (KCP&L)
MidAmerican Energy Company
Progress Energy (PGN)
Southern Company
Westar 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)