

CAN-0024 Comment Analysis Summary

CIP-002 R3 Routable Protocols and Data Diode Devices

CAN-0024 provides instruction for assessing whether the communication characteristics of data diode devices can be used to exclude non-critical Cyber Assets from consideration as Critical Cyber Assets (CCA) when a routable protocol is used. The CAN was posted for industry comment on the NERC web site on October 10, 2011 and the comment period expired on October 31, 2011. NERC received 21 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, scope and the effective date of the CAN.

Errata

The recommended errata changes were implemented in order to provide clarity in the CAN. Such changes that were made include removing “non-critical” from the issue statement and adding the term “essential” in the first paragraph. Also, Critical Assets and Cyber Assets were spelled out and all references to the acronym “CA” were removed to eliminate any confusion.

Scope

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

Several commenters stated that a CAN was not the proper vehicle to introduce a defined term of “data diode device,” as the NERC Standards Development Process is more suitable for introducing defined terms. In response to this comment, data diode devices have caused confusion during compliance monitoring and presented a potential area for inconsistent application of the standard across the ERO. CAN-0024 does not define “data diode device” in a way that suggests it should be added to the NERC Glossary of Terms, but rather as a description to describe the technical attributes of the devices and provide guidance to Compliance Enforcement Authority (CEA) staff when they are applying the standard in the field.

Another comment received regarded the Cyber Assets at control centers, which stated that the CAN did not address CIP-002 R3.2. In response, CAN-0024 only applies to Cyber Assets not located at control centers. The external communication characteristics of Cyber Assets at control centers have no bearing on whether the associated Cyber Assets should be determined to be Critical Cyber Assets.

NERC also received several technical comments on the connectivity of the devices. In response to those comments, a section was added in the background section of CAN-0024 that instructs CEAs to assess connectivity by differentiating embedded devices from stand-alone devices. The purpose of this CAN is to provide the requisite information to CEA staff so they have guidance on how to assess

compliance with different configurations. However, the compliance assessment will be based on whether a Cyber Asset uses a routable protocol to communicate outside the ESP,

Effective Date

Several commenters believe that NERC should incorporate a reasonable implementation period of 12 months for CAN-0024 to allow affected entities sufficient time to evaluate their system and install a perimeter security device if necessary. However, this CAN reiterates the clear language of the standard – “*The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter*”, and therefore the effective date of CAN-0024 is date of that the CAN is posted as final on the NERC web site. CEAs will apply discretion in applying the compliance application for registered entities that have had an audit initiated.

Conclusion

The analysis spreadsheet for CAN-0024 is posted on the NERC website. Because the spreadsheet format may not provide sufficient visibility into the effort that NERC puts into reviewing all of the comments received with respect to this CAN, this document is intended to supplement that information. NERC staff thanks industry for the time and effort put into providing that feedback. If you would like further discussion on CAN-0024, please feel free to contact us at cancomments@nerc.net.

Registered Entities that submitted CAN Comments

Ameren

American Electric Power (AEP)

Arizona Public Service Company (AZPS)

Associated Electric Cooperative, Basin Electric Power Cooperative and Tri-State Generation and Transmission Association (G&T Cooperatives)

Bonneville Power Administration (BPA)

Central Lincoln

Chelan County Public Utility District

Dominion Resources Services, Inc.

Entergy

Kansas City Power & Light (KCP&L)

Manitoba Hydro

MidAmerican Energy Company

Nebraska Public Power District

Northeast Utilities (NU)

Oncor Electric Delivery Company

Pepco Holdings, Inc. (PHI)

PNM Resources

PSEG Services Corporation

San Diego Gas & Electric (SDG&E)
Western Area Power Administration

Trade Associations that submitted CAN Comments

Edison Electric Institute (EEI)

ISO/RTO Council Standards Review Committee (IRC SRC)

Midwest Reliability Organization NERC Standards Review Forum (MRO NSRF)

National Rural Electric Cooperative Association (NRECA)