

Compliance Application Notice — 0024

CIP-002 ~~CIP-009~~_R3 Routable Protocols and Data Diode Devices

Posted ~~[DATE]~~ December 15, 2011

Primary Interest Groups

Compliance Enforcement Authority (CEA)¹
NERC
Regional Entity (RE)
Reliability Coordinator (RC)
Transmission Owner (TO)
Transmission Operator (TOP)
Balancing Authority (BA)
Generator Owner (GO)
Generator Operator (GOP)
Load Serving Entity (LSE)
Interchange Authority (IA)
Transmission Service Provider (TSP)

Issue: Can communication characteristics of data diode devices allow a Cyber Asset to be excluded from NERC Critical Infrastructure Protection (CIP) Standards?

For the purpose of aiding a CEA, this CAN 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 ~~implemented~~ used when not at a control center.

CAN Summary

CEAs are to verify whether a registered entity has properly identified CCAs when a routable protocol is ~~implemented~~ used. CEAs are instructed to find that ~~, because~~ data diode devices that use routable protocols cannot be used as a rationale in the methodology of designating CCAs to exclude assets from compliance with CIP standards.

Note that this CAN 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.

¹ Compliance Enforcement Authorities include ERO auditors, investigators, enforcement personnel or any person authorized to assess issues of concern, potential non-compliance, and possible, alleged or confirmed violations of NERC Reliability Standard requirements.

Background

CIP-002 (~~versions 1, 2 and 3~~) requires the identification of ~~essential~~ Critical Assets and associated ~~essential Cyber Assets as~~ CCAs. CIP-002 R3.1 provides that a Cyber Asset ~~associated-essential to the operation of~~ with a Critical Asset (~~and not at a control center~~) ~~to~~ must be designated a CCA if it uses a routable protocol² to communicate outside the Electronic Security Perimeter (ESP).

Data diode devices provide a ~~hardware-enforced~~ “one-way” (uni-directional) path for data to flow across the ESP. Several commercial products are available that perform this function, each of which operates in a slightly different way from the others. However, nearly all commercially available stand-alone data diode devices provide for connectivity to IP networks on each side of the stand-alone data diode device. This IP connectivity is assumed to be implemented primarily to minimize the impact to the “internal” Cyber Assets. It is further assumed that, in the context of the CIP standards, the stand-alone data diode devices will be implemented to transmit data from the CCA portion of the network to the “outside” portion of the network in a write-only direction from the CCA portion of the network.

An ~~easy~~ way to assess ~~this~~ ~~the connectivity~~ is to determine if the network interfaces on the stand-alone data diode device are configured with IP addresses. If the stand-alone data diode device has one or more IP addresses, it is “using” a routable protocol for communication.

Another type of data diode device consists of network interface cards that are installed into existing Cyber Assets, and which provide the same uni-directional communication as stand-alone data diode devices. For the purpose of this CAN, these will be referred to as “embedded data diode devices” to distinguish them from stand-alone data diode devices. ~~In this case, the data does not use a routable connection to cross the ESP, and the Cyber Assets do not meet the connectivity requirement.~~
~~Since data diode devices can only transmit data in a single direction, normal flow control that is typically handled by the TCP layer in a TCP/IP network cannot be accomplished. The sending Cyber Asset cannot guarantee that the receiving Cyber Asset has received the data. If the data is relied upon for essential functions such as control systems, this lack of communication status feedback may be unacceptable.~~

~~Similarly, most control systems require not only the transmission of data, but also the receipt of data requests and control commands. A data diode device implemented in a write-only direction as an ESP access control point will not allow data requests, control commands, communication status feedback or set points from external supervisory systems such as SCADA systems.~~

Compliance Application

CIP-002-~~3~~ R3 provides, in pertinent part:

***R3. Critical Cyber Asset Identification** — using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as*

² The most commonly implemented example of a routable protocol is IP (Internet Protocol). Other routable protocols exist, notably the OSI protocol, but the use of these other routable protocols is extremely limited in North America.

necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,...

R3.3. The Cyber Asset is dial-up accessible.

NERC Reliability Standard CIP-002 requires the identification of Critical Assets and associated CCAs. The plain language of CIP-002 R3.1 does not discuss directionality of data flow—only whether the Cyber Asset communicates to external systems (to communicate outside the Electronic Security Perimeter) using a routable protocol.

Therefore, under ~~the current version of the CIP Standards standards~~ sub-requirement of R3.1, the relevant criteria for determining whether non-critical Cyber Assets are to be classified as CCAs is the use of a routable protocol to communicate outside the Electronic Security Perimeter (when not at a control center). Stand-alone data diode devices receive and transmit data through an IP network, which is a routable protocol.

~~Therefore, despite the use of these devices, the CAs that uses a routable protocol to communicate either outside the ESP must be identified as a CCAs. The use of a routable protocol to communicate to Cyber Assets outside the ESP or within a control center will subject these assets to CIP Standards as CCAs. Therefore, a CEA is to find a Possible Violation when a registered entity does not identify a Cyber Asset that uses a routable protocol to communicate outside the ESP, regardless of whether that routable communication is direct through a firewall, or indirect using a stand-alone data diode device. The “use” of a routable protocol to communicate to Cyber Assets outside the ESP will subject these assets to CIP Standards as CCAs.~~

Effective Period for CAN

This CAN is effective upon posting as final on the NERC Web site, and 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. It supersedes all prior communications and will remain in effect until such time that a future version of a FERC or other applicable government authority approved standard or interpretation becomes effective and addresses the specific issue contained in this CAN.

For any enforcement action in process and for audits that have been initiated,³ 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.

Providing Evidence of Compliance

A CEA is to consider the following to obtain reasonable assurance of the entity’s compliance:

- Evidence of the registered entity’s assessment as to whether a Cyber Asset not located at a control center was determined to be a CCA, based upon whether the Cyber Asset:

³ “Initiated” means that a registered entity has received notification of the upcoming audit.

- is associated with a Critical Asset,
- is essential to the reliable operation of the Critical Asset, and
- meets the connectivity qualification described in CIP-002 R3.1, ~~R3.2~~ and R3.3 (e.g., uses routable protocols to communicate to Cyber Assets outside the Electronic Security Perimeter ~~(R3.1) or within a control room (R3.2), or is dial-up accessible (R3.3)~~).

If the Cyber Asset was deemed not to be a CCA, the CEA should verify whether that:

- no routable protocols were used to communicate to Cyber Assets outside the ESP; and
- the cyber asset is not dial-up accessible.

For more information please contact:

Michael Moon
Director of Compliance Operations
michael.moon@nerc.net
404-446-2567

Valerie Agnew
Manager of Interface and Outreach
valerie.agnew@nerc.net
404-446-2566

Ben Engelby
Senior Compliance Specialist
ben.engelby@nerc.net
404-446-2578

This document is designed to convey compliance monitoring instruction to achieve a measure of consistency among auditors and Compliance Enforcement Authorities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing NERC Reliability Standard. Compliance will continue to be assessed based on language in the currently enforceable NERC Reliability Standards. This document is not intended to define the exclusive method an entity must use to comply with a particular standard or requirement, or foreclose a registered entity's demonstration by alternative means that it has complied with the language and intent of the standard or requirement, taking into account the facts and circumstances of a particular registered entity. Implementation of information in this document is not a substitute for compliance with requirements in NERC's Reliability Standards.