

CAN Comment Form Compliance Application Notice – 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Brandy A. Dunn

Phone Number: 720-962-7431

Email Address: dunn@wapa.gov

Entity Represented: Western Area Power Administration

Region: WECC

Primary Interest Groups

Are you suggesting a change to the groups mentioned? Yes / No

If yes, explain what change and why:

No

Issue

Are you suggesting a change to the issue statement of the CAN? Yes / No

If yes, explain what change and why:

Yes – The attempt to address the issue outlined in the statement exceeds the CIP-002-3, R3 standard. Also, Western does not consider the term “data diode” an industry standard term and it is not defined in sufficient detail. This would make application of a consistent interpretation by all CEAs unlikely, making this CAN inappropriate for use in any audit or enforcement action. Should an Entity choose to use “data diodes” terminology, their devices should be addressed (justified) in the relevant their assessment method for determining CCAs per CIP-002-3, R3; not in a CAN based on assumption of how these devices are determined or used.

Background

Are you suggesting a change to the background statement of the CAN? Yes / No

If yes, explain what change and why:

Yes – The CAN statement attempts to expand CIP requirements with *assumption* of how devices are currently implemented and used by all entities. Therefore, Western suggests, at a minimum, removal of the following language:

“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.”

“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

Are you suggesting a change to the compliance application section of the CAN? Yes / No

If yes, explain what change and why:

Yes, at a minimum as follows:

“Therefore, under the current subrequirement of R3.1, the relevant criteria for determining whether non-critical CAs are to be classified as CCAs is the use of a routable protocol to communicate outside the Electronic Security Perimeter. ~~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 use a routable protocol to communicate outside the ESP must be identified as CCAs.~~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

Are you suggesting a change to the effective period of the CAN? Yes / No

If yes, explain what change and why:

Yes –

- 1) This Compliance Application Notice should not become effective as it exceeds the established requirements of CIP-002-3, R3.
- 2) There is no implementation plan.

Evidence of Compliance

Are you suggesting a change to the evidence of compliance mentioned in the CAN? Yes / No

If yes, explain what change and why:

No – the evidence is the same for the standard in effect

CAN Comment Form

CAN Number 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Steve Alexanderson

Phone Number: 541-574-2064

Email Address: salexanderson@cencoast.com

Entity (ies) Represented: Central Lincoln

Region(s): WECC

Primary Interest Groups

Do you disagree with the groups mentioned? No

If yes, explain why:

Issue

Do you disagree with the issue statement of the CAN? Yes

If yes, explain why:

The issue statement suggests a cyber asset can simultaneously be considered non-critical and critical. Suggest removing the word non-critical:

“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 Cyber Assets from consideration as Critical Cyber Assets (CCA) when a routable protocol is implemented.

Background

Do you disagree with the background statement of the CAN? Yes

If yes, explain why:

The CAN classifies data diodes as "stand alone" and "embedded" and proceeds to do a great job of explaining how the standalone devices are to be treated. Please provide a similar treatment for the embedded devices. The one statement suggesting the treatment of the embedded devices was removed: "In this case, like that using a legacy connection, the data does not use a routable connection to cross the ESP."

The statement: "...the relevant criteria for determining whether non-critical CAs are to be classified as CCAs is the use of a routable protocol..." leads to a possible oxymoron where a cyber asset is simultaneously non-critical and critical. Suggest removing the word non-critical. "Criteria" is plural while "is" is singular. We suggest using the singular form. We note that the acronym CA is not defined here, but is commonly used to mean "Critical Asset" From the context, we believe the author meant it to mean "Cyber Asset," so we suggest spelling the words out:

"Therefore, under the current subrequirement of R3.1, the relevant criterion for determining whether Cyber Assets are to be classified as CCAs is the use of a routable protocol to communicate outside the Electronic Security Perimeter."

Compliance Application

Do you disagree with the compliance application section of the CAN? No
If yes, explain why:

Effective Period for CAN

Do you disagree with the effective period of the CAN? No
If yes, explain why:

Evidence of Compliance

Do you disagree with the evidence of compliance mentioned in the CAN? No
If yes, explain why:

CAN Comment Form

Compliance Application Notice – 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Jesse Halpern
Phone Number: 202.296.1500
Email Address: jyhalpern@brudergentile.com
Entity Represented: Associated Electric Cooperative, Inc., Basin Electric Power Cooperative, Inc., and Tri-State Generation and Transmission Association, Inc.
Region: SERC, MRO, and WECC, respectively

Associated Electric Cooperative, Inc. (“Associated”), Basin Electric Power Cooperative, Inc. (“Basin Electric”), and Tri-State Generation and Transmission Association, Inc. (“Tri-State”) (collectively, the “G&T Cooperatives”) respectfully submit these comments on the North American Electric Reliability Corporation’s (“NERC”) draft Compliance Application Notice (“CAN”) CAN-0024, which was posted for industry review and comment on Friday, May 20, 2011 and again on October 10, 2011. NERC has proposed guidance to clarify “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.” NERC’s proposal contains several technical inaccuracies that should be addressed before the CAN is finalized. The CAN also goes beyond the proper scope of a CAN because it attempts to alter the definition of Critical Cyber Assets under CIP-002-3 and creates new requirements concerning the use of data diode devices in control system settings.

Primary Interest Groups

Are you suggesting a change to the groups mentioned? No
If yes, explain what change and why:

Issue

Are you suggesting a change to the issue statement of the CAN? No

If yes, explain what change and why:

Background

Are you suggesting a change to the background statement of the CAN? Yes

If yes, explain what change and why:

The second through sixth paragraphs of the “Background” section should be deleted. Please see the discussion under the “Compliance Application” section below for a detailed explanation.

Compliance Application

Are you suggesting a change to the compliance application section of the CAN? Yes

If yes, explain what change and why:

I. NERC SHOULD REVISE CAN-0024 TO ADDRESS THE TECHNICAL INACCURACIES AND DIFFERENTIATE BETWEEN ROUTABLE AND NON-ROUTABLE IMPLEMENTATIONS OF DATA DIODES.

CAN-0024 contains technical inaccuracies concerning the implementation and use of data diodes that should be corrected prior to the finalization of the CAN. CAN-0024 states that data diodes cannot be used to exclude Critical Cyber Assets from compliance with the Critical Infrastructure Protection (“CIP”) Standards when a routable protocol is implemented. This statement fails to recognize that data diodes may be configured and implemented using a variety of options, including options that can provide protection to Critical Cyber Assets. While data diodes may be configured as TCP/IP proxies that appear to permit a routable protocol to communicate outside of the Electronic Security Perimeter, draft CAN-0024 overlooks the industry-recognized technical value of data diode devices: they are one-way communication devices by design. Data diode devices are designed to protect a network’s integrity or

confidentiality from unauthorized access and cyber attacks. As a result, while data diode devices may receive data from or transmit data to a connected IP network (a routable protocol), they are designed to permit only uni-directional traffic and prevent users from exploiting the routable protocol.¹ Therefore, data diodes can be configured in a way that justifies excluding Cyber Assets from CIP compliance. As a result, the G&T Cooperatives urge NERC to revise the draft CAN to recommend that the Registered Entity and NERC consider both the manufacturer’s design specifications and the options selected in the configuration and implementation of data diodes when determining whether or not the Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter or within a control center and therefore should be classified as a Critical Cyber Asset. NERC also should consider providing additional guidance requiring that each Electronic Security Perimeter should have its data diodes’ uni-directional paths oriented in a single direction, either all outward or all inward.

Further, CIP-002-3 does not classify Cyber Assets located within an Electronic Security Perimeter that use a “serial, non-routable” connection to communicate outside of that Electronic Security Perimeter as Critical Cyber Assets. Serial, non-routable connections provide only point-to-point (but two-way, *i.e.*, read & write, up & down) communication that is considered low risk. Data diodes are able to provide superior protection to the Cyber Assets within an Electronic Security Perimeter by preventing any inbound communications. There is no “write up” of data, which in turn ensures the integrity of the data/devices within the Electronic Security Perimeter. As a result, correctly configured

¹ Draft CAN-0024 mistakenly suggests that a data diode automatically uses a routable protocol if it has an IP address. However, by definition, a routable protocol is a *communications protocol* that contains a network address as well as a device address and allows packets to be forwarded from one network to another. A communications protocol sends and receives packets containing routing information to and from other devices. When a data diode is configured to permit uni-directional communications only (either sending or receiving packets of information), it does not meet the definition of a routable protocol.

data diodes are more secure than serial, non-routable connections and can be used to provide equivalent or superior protection to data and devices contained within the Electronic Security Perimeter. Therefore, the G&T Cooperatives request that NERC revise the draft CAN to acknowledge the uniqueness of the data diode's "one-way" communication channel, and provide guidance concerning the circumstances in which data diode devices can be used to provide access to information and offer the same protection (and benefits) as serial, non-routable connections.

Finally, CAN-0024 incorrectly implies that a data diode would be unable to restrict communications across a path that would otherwise be considered a routable protocol. A routable protocol contains a network address as well as a device address, allowing packets to traverse disparate networks. In contrast, a non-routable protocol contains only a device address and not a network address. It does not incorporate an addressing scheme for routing data from one network to another. As a result, a data diode implementation that permits only one-way communication via a device addressing design would restrict the flow of data, effectively instituting a non-routable protocol. NERC should revise the final paragraph of the "Compliance Application" section of the draft CAN to acknowledge that the use of a data diode can serve to determine whether a communications path across an Electronic Security Perimeter is routable or non-routable.

II. NERC SHOULD REVISE CAN-0024 TO ENSURE THAT IT DOES NOT IMPROPERLY ESTABLISH NEW REQUIREMENTS.

A. NERC CANNOT ESTABLISH NEW RELIABILITY REQUIREMENTS THROUGH CANS.

NERC can establish reliability requirements only through the issuance of reliability standards. Federal Power Act ("FPA") Section 215 requires that "[t]he Electric Reliability Organization shall file

each reliability standard or modification to a reliability standard that it proposes to be made effective under this section with the Commission.”² Pursuant to FPA Section 215, NERC is required to follow the Standards Development process and obtain FERC approval prior to enacting new Reliability Standards or modifying existing Reliability Standards.

NERC cannot implement new standards through the issuance of CANs. Consistent with FPA Section 215, NERC notes in each CAN that “The document is designed to convey compliance guidance from NERC’s various activities. It is not intended to establish new requirements under NERC’s Reliability Standards or modify the requirements in any existing NERC Reliability Standard.” NERC also states that CANs are to assist NERC’s Compliance Operations, Regional Entities and Registered Entities with compliance by providing consistency and transparency.³

B. CAN-0024 IMPROPERLY ATTEMPTS TO REVISE THE DEFINITION OF A CRITICAL CYBER ASSET.

CAN-0024 improperly attempts to revise the definition of a Critical Cyber Asset by expanding it to non-critical Cyber Assets located within the Electronic Security Perimeter that use routable protocols to communicate outside the Electronic Security Perimeter. Specifically, the “Compliance Application” section of draft CAN-0024 states that

the relevant criteria for determining whether non-critical CAs are to be classified as CCAs is the use of routable protocol to communicate outside the Electronic Security Perimeter. . . . The use of a routable protocol to communicate to Cyber Assets outside the ESP will subject these assets to CIP Standards as CCAs.

² 16 U.S.C. § 824o(d) (2006).

³ “Compliance Application Notices,” available at <http://www.nerc.com/page.php?cid=3|22|354>.

This conflicts with the plain language of the reliability standard, which provides that Critical Cyber Assets are those Cyber Assets that are “essential to the operation of the Critical Asset” and meets 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.

Therefore, based on the plain language of CIP-002-3 R3, to be considered a Critical Cyber Asset, a device must (1) be essential to the operation of a Critical Asset identified under CIP-002-3 R2 and (2) meet one of the three characteristics listed above (use a routable protocol to communicate outside the Electronic Security Perimeter, use a routable protocol within a control center, or be dial-up accessible). Contrary to the implications of draft CAN-0024, if a device does not meet both criteria it is not a Critical Cyber Asset under CIP-002-3. It would, however, be identified as a non-critical Cyber Asset and afforded the protections identified in CIP-005-3. Consequently, NERC should revise the “Compliance Application” section of draft CAN-0024 to clarify that only those Critical Assets that are essential to operation of a Critical Asset identified under CIP-002-3 R2 and that use a routable protocol to communicate outside of an Electronic Security Perimeter or within a control center should be identified as Critical Cyber Assets.

C. CAN-0024 IMPROPERLY ATTEMPTS TO IMPOSE NEW REQUIREMENTS PROHIBITING THE USE OF DATA DIODES IN A CONTROL SYSTEM SETTING.

CAN-0024 improperly proposes to implement new requirements relating to the transmission and receipt of data by control systems. Specifically, the second through sixth paragraphs of the

“Background” section attempt to specify how control systems must communicate with other devices such as external supervisory systems (*e.g.*, SCADA systems). The CIP reliability standards do not include requirements governing the manner in which control systems must communicate with one another, so this is not a clarification of an existing rule or requirement. In addition, rather than clarifying whether data diodes’ communication characteristics allow a Cyber Asset to be excluded from CIP compliance, these Background paragraphs address the technical merits of implementing data diode devices in control systems, stating that because “data diode devices can only transmit data in a single direction, . . . [t]he sending Cyber Asset cannot guarantee that the receiving Cyber Asset has received the data” and, due to the essential nature of the systems, this “may be unacceptable.” These paragraphs are based on generalities that do not recognize that data diodes may be configured and implemented using a variety of options to meet the communication and feedback requirements of individual control systems. Further, NERC’s suggestion that the data diodes’ uni-directional path for data to flow across an Electronic Security Perimeter compromises data availability and integrity is misplaced. Data diodes can provide the required bi-directional TCP/IP handshakes for their independently networked terminals and simultaneously prevent two-way communications between those terminals. In other words, a data diode may act as a TCP/IP proxy by wrapping a payload sent from a sender to a receiver. Thus, data diodes can be used in real-time data monitoring to validate the timeliness and accuracy of the data, provided that certain design considerations are implemented to address the circumstances. Moreover, using a short fiber-optic cable, an optic transmitter, and an optic receiver, the uni-directional connection across a data diode can far exceed the reliability of a LAN or WAN network, so the use of packet acknowledgement across the data diode interface is typically unnecessary from a practical standpoint. Nonetheless, industry engineers understand that because data diodes are designed to provide one-way

communications, they generally are not appropriate for use in communication paths where there is a need for closed-loop control.

As noted above, the second through sixth paragraphs of the “Background” section are unrelated to the ostensible purpose of CAN-0024, which is to clarify “whether the communication characteristics of data diode devices can be used to exclude non-critical Cyber Assets (CA) from consideration as Critical Cyber Assets (CCA) when a routable protocol is implemented, thereby making them inapplicable to CIP Standards.” Since draft CAN-0024 creates new requirements prohibiting the use of data diodes in a control system setting, it exceeds the permissible scope of a CAN. Consequently, these paragraphs should be deleted.

Effective Period for CAN

Are you suggesting a change to the effective period of the CAN? No

If yes, explain what change and why:

Evidence of Compliance

Are you suggesting a change to the evidence of compliance mentioned in the CAN? No

If yes, explain what change and why:

CAN Comment Form Compliance Application Notice – 00

Please complete the CAN Comment Form and email it to cancomments@nerc.net. Due to the amount of comments NERC receives, we will not accept attachments or comments submitted in another format.

Commenter Information

Name:

Phone Number:

Email Address:

Entity (ies) Represented:

Region(s):

Primary Interest Groups

Do you disagree with the groups mentioned? Yes or No

If yes, explain why:

Issue

Do you disagree with the issue statement of the CAN? Yes or No

If yes, explain why:

Background

Do you disagree with the background statement of the CAN? Yes or No
If yes, explain why:

Compliance Application

Do you disagree with the compliance application section of the CAN? Yes or No
If yes, explain why:

Effective Period for CAN

Do you disagree with the effective period of the CAN? Yes or No

If yes, explain why:

Evidence of Compliance

Do you disagree with the evidence of compliance mentioned in the CAN? Yes or No

If yes, explain why:

CAN Comment Form

Compliance Application Notice – 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Chad Bowman

Phone Number: (509) 661-4605

Email Address: chad.bowman@chelanpud.org

Entity Represented: Public Utility District No. 1 of Chelan County (CHPD)

Region: WECC

Primary Interest Groups

Are you suggesting a change to the groups mentioned? No

If yes, explain what change and why:

Issue

Are you suggesting a change to the issue statement of the CAN? Yes

If yes, explain what change and why:

This statement addresses the characteristics of “data diodes,” a term that is not included in the NERC Glossary of Terms or in the standard. We respectfully submit that it is not the role of a CAN to define terms and request that this CAN be held until the term “data diode” can be defined by processes outlined in the Standards Processes Manual.

Background

Are you suggesting a change to the background statement of the CAN? No

If yes, explain what change and why:

Compliance Application

Are you suggesting a change to the compliance application section of the CAN? No

If yes, explain what change and why:

Effective Period for CAN

Are you suggesting a change to the effective period of the CAN? Yes

If yes, explain what change and why:

This CAN should not be implemented until the term “data diodes” has been clearly defined.

Evidence of Compliance

Are you suggesting a change to the evidence of compliance mentioned in the CAN? No

If yes, explain what change and why:

CAN Comment Form

Compliance Application Notice – 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Christine Hasha

Phone Number: (512) 248-3909

Email Address: src@misoenergy.org

Entity Represented: IRC Standards Review Committee (SRC)

Region: The SRC is comprised of the Alberta Electric System Operator (“AESO”), Electric Reliability Council of Texas (“ERCOT”), the Independent Electricity System Operator of Ontario, Inc. (“IESO”), ISO New England, Inc. (“ISO-NE”), Midwest Independent Transmission System Operator, Inc. (“Midwest ISO”), New York Independent System Operator, Inc. (“NYISO”), PJM Interconnection, L.L.C. (“PJM”), Southwest Power Pool, Inc. (“SPP”), New Brunswick System Operator (“NBSO”), and California ISO (“CA ISO”). AESO abstains from these comments.

Primary Interest Groups

Are you suggesting a change to the groups mentioned? No

If yes, explain what change and why:

Issue

Are you suggesting a change to the issue statement of the CAN? Yes

If yes, explain what change and why:

As written, the CAN presents the guidance as governing and enforceable. Since the CAN is not enforceable, the SRC offer the following changes to the language: “For the purpose of aiding a CEA, this CAN provides **guidance** for **understanding** 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.”

With regards to the **CAN Summary** section, the SRC takes exception to the following language. “CEAs are instructed to find that data diode devices that use routable protocols cannot be used to exclude assets from compliance with CIP standards as CCAs.” The CAN language substantively changes the

explicit requirements of CIP-002 R3.1. The language also leaves out a very important element of R3, “the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset.” This language provides clear direction of how to apply the requirement without due consideration of the assets in question and the methodologies utilized by the Responsible Entity to identify the assets essential to the operations of the Critical Asset. The CAN creates a requirement where the Responsible Entity has been clear discretion to determine what is critical. This language should be removed.

Background

Are you suggesting a change to the background statement of the CAN? Yes
If yes, explain what change and why:

The CAN language substantively changes the explicit requirements of CIP-002 R3.1. The language also leaves out a very important element of R3, “the Responsible Entity shall develop a list of associated Critical Cyber Assets *essential to the operation* of the Critical Asset.” The CAN language provides clear direction of how to apply the requirement without due consideration of the assets in question and the methodologies utilized by the Responsible Entity to identify the assets essential to the operations of the Critical Asset. The CAN creates a requirement where the Responsible Entity has been clear discretion to determine what is critical. This language should be removed.

The CIP standards were developed and are in place to promote physical and electronic security for critical assets and critical cyber assets. CAN-0024 blurs the line between security and IP network reliability by introducing network transmission flow control requirements that were developed to confirm data transmission reliability from one node to another. It is NOT intended as a security function, and is therefore beyond the scope of CIP. Other standards, COM-001 for example, are in place to provide requirements related to network redundancy and reliability, and if additional enhancements are sought, then the standards drafting process should be utilized.

Also, CIP-005, R2.4 speaks specifically about external interactive access into the ESP (from outside the ESP) as a necessary security control point when interactive access is enabled. In simple terms, that means that if a person establishes a connection across the ESP, then additional security controls must be in place. This not only implies that non-interactive sections are permissible, but it also clearly depicts mechanisms used to protect connections flowing in a single direction (inbound). A precedent has been set that governs data flow in a single direction. Therefore, the fifth paragraph (next to last) on the second page of CAN-0024 is not entirely accurate, as CIP-005, R2.4 absolutely defines the “directionality of data flow”. This definition is pertinent to this CAN.

CAN-0024 also depicts single direction data transmissions as somehow unreliable and “may be unacceptable” because the “sending Cyber Asset cannot guarantee that the receiving Cyber Asset has received the data.” (See second paragraph, page 2). The Transport Layer of the TCP/IP (network protocol) model includes the User Datagram Protocol (UDP), which is connectionless in nature. This simply means that while UDP is a part of the Internet Protocol Suite (the “IP” in TCP/IP), it also lacks reliability as it does not confirm the proper delivery of data from one node to another. Are we then to descend further down this slippery slope to determine that UDP is an unacceptable protocol since it also lacks typical network “handshaking” and error checking?

NERC should absolutely NOT be making this type of significant interpretation via a CAN in any standards, much less the CIP standards. Ironically, data diodes were designed with one-way data transmission capabilities to enhance security capabilities. It is important to note that the CAN will then apply additional scrutiny to the use of these diodes within the ESP because of a perceived lack of reliability, and because of possible peripheral connections.

CAN-0024 directly conflicts with “Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets” which was approved by the CIPC and is dated June 17, 2010, and with the original CIP FAQs provided by NERC (CIP-002-009_FAQs_11Jan06.pdf) whereby “routable protocol” is defined as operating at Layer 3 or higher on the OSI model. Data diodes do NOT operate at layer 3 or higher unless additional, secondary connections are added/configured in that fashion. Finally, once the entire CAN-0024 is contemplated, the only thing that establishes the CCA applicability is not the uni-directional data transmission, but other possible TCP/IP based connections that may also exist on the diode. This deals solely with diode setup/configuration, and not the transport mechanism.

CAN-0024 should not be enacted, and data reliability comments should be left for white papers and perhaps NERC guidelines only.

Compliance Application

Are you suggesting a change to the compliance application section of the CAN? Yes
If yes, explain what change and why:

Please see the prior comments within this form. The CAN creates a clear requirement that is not currently supported by the wording of CIP-002 R3 without due consideration of what is essential. The CAN is looking at a single subrequirement without the context of the overall governing requirement. Furthermore, the CAN adopts an approach that is directly inapposite to previously provided guidance by expanding the definition of routable protocol to devices that do not operate at Layer 3 or higher on the OSI model. Further, the CAN presents an overly loose interpretation of what it means to “use a routable protocol” in which the capability of using a routable protocol is interpreted as the use of a routable

protocol. In application, this CAN could have a negative impact on reliability by calling the use of uni-directional communications into question and potentially stifling important industry initiatives like current synchrophasor projects as it raises a question as to whether data collection devices, such as Phasor Measurement Units, would become CCAs.

Effective Period for CAN

Are you suggesting a change to the effective period of the CAN? Yes
If yes, explain what change and why:

By using phrases such as “are to use this CAN to assess compliance” and “apply appropriate discretion,” the “Effective Period” section implies that the guidance provided in the CAN is mandatory, despite the fact that the CAN is not developed through the Standards Development Process, not balloted and not approved by government authorities. The SRC recommends not using the terms “compliance,” “non-compliance,” or “assess,” or “assessment.”

Evidence of Compliance

Are you suggesting a change to the evidence of compliance mentioned in the CAN? Yes
If yes, explain what change and why:

Please see the prior comments within this form. The CAN creates a clear requirement that is not currently supported by the wording of CIP-002 R3 without due consideration of what is essential.

The comments listed within this email are for the following registrations:

NCR01234 – Entergy
NCR10226 – Llano Estacado Wind LP
NCR01094 – Entergy Power
NCR01019 – Northern Iowa
NCR07071 - Entergy Nuclear Fitzpatrick, LLC.
NCR07072 - Entergy Nuclear Generation Company
NCR07073 - Entergy Nuclear Indian Point 2, LLC.
NCR07074 - Entergy Nuclear Indian Point 3, LLC.
NCR07075 - Entergy Nuclear Vermont Yankee, LLC.
NCR08052 - Entergy Nuclear Palisades, LLC.

The comments are as follows:

If a data diode is used as the access point to an ESP, the devices inside would only be using a routable protocol to communicate *within* the ESP. Data Diodes use non-routeable, physically limited to one-way (inside to outside) communication mechanisms to communicate outside the ESP. Yes, routeable communication exist within the ESP; and yes, routeable communications exist outside the ESP; but no routeable communications traverse the ESP Access Point.

In fact, *it is impossible to use a routeable protocol* to communicate from the inside to the outside of a data-diode, and *you cannot communicate at all from the outside to the inside*. Therefore, the threat of external attack is zero when using a data diode (provided of course our understanding of the laws of physics hold) yet those devices would be considered CCAs. If an organization uses some sort of serial connection, the threat of external attack, however low, is greater than zero, yet those devices would not be considered CCAs.

Please let us know if you have any questions or comments.

Thank you,

Nacy Mille
Entergy

**EEI Comments on
CAN-0010, CAN-0011, CAN-0012,
CAN-0013, CAN-0015, CAN-0022,
CAN-0024, CAN-0026, and CAN-0028
October 31, 2011**

On behalf of our member companies, the Edison Electric Institute (EEI) appreciates the opportunity to provide the following comments on proposed Compliance Application Notices (CANs) 0010, 0011, 0012, 0015, 0022, 0024, 0026 and 0028.

General Comments

EEI acknowledges and appreciates the recent posting of the CAN Process document as well as the final reposting of CAN-0016, however we continue to have five general concerns. First, NERC continues to propose CANs that are, in fact, interpretations of approved Reliability Standard Requirements. NERC expressly states that CANs do not and should not establish new requirements under the FERC-approved Reliability Standards and EEI urges NERC to hold to this basic policy principle. Furthermore, EEI respectfully suggests that NERC ought to reinforce to CEAs, as a routine part of their compliance guidance that CANs should not be considered as the sole method of attaining compliance. Companies recognize that there are often multiple ways for an entity to comply with a standard and in many cases requirements do not specifically define relevant terms or processes, thereby allowing a broad range of solutions that an entity might achieve an equal level of compliance. Therefore, we believe that NERC's desire for more uniform enforcement must be tempered within the bounds of the plain language of the standard and ask that compliance authorities seek to avoid the pitfalls of rigid compliance guidance, which often lead to interpretations that introduce new problems while solving old ones.

Second, EEI believes that NERC needs to incorporate a reasonable implementation period for all CANs. Generally, we have observed that CANs routinely apply either retroactive enforcement or enforcement from the point of "Final Posting". In both cases, entities are not afforded any ability to adjust their programs, policies, systems or hardware to conform to these newly defined or clarified requirements. This approach, if left unchanged, will ensure that many, if not most, registered entities will be continually self reporting their potential non-compliance as a result of CANs. This situation is troubling particularly at a time when NERC is pursuing Find, Fix, Track and Report as a way to redirect compliance resources to those issues that pose the greatest risk to Bulk Power System reliability.

EEI believes that prior to developing a CAN, NERC should exercise more discernment when considering stakeholder questions, and CAN candidate topics for CANs, and limit compliance direction to those questions that have clear merit. Within this current group of CANs we again find issues or questions that lack substantive technical merit. For example, TOP-006 R1.2 provides clear language regarding the obligations of Transmission Operators and Balancing Authorities, yet NERC still feels compelled to develop a CAN to restate what we believe to be

clear and unambiguous language. Examples such as this continue to diminish the credibility of the CANs process and raise the question, whether NERC should attach the original question to all issued CANs. This approach might help companies better understand the context of the original question as well as improve our ability to provide relevant comments.

Fourth, we continue to believe that the CANs process would be better served by holding firm to the premise that CANs should be clear, concise, and to the point; focused solely on clarifying the issue raised and strictly avoiding areas where no compliance concerns have been identified or raised. We also note that this batch of proposed CANs also contains difficult to understand language and reasoning.

Finally, EEI notes that in this new batch of proposed CANs NERC did not consistently identify the Reliability Standard version for which the CAN was written and on occasion did not include the specific requirement in question. We believe omissions of this type, over time; will result in CANs that exist but simply do not match the version of the standard for which they were originally written as well as diminish focus on the requirement that is in question.

Specific Compliance Application Notice Comments

CAN-0010

Reliability Standard Referenced:

N/A

Reliability Standard Title(s):

N/A

Requirement(s) Identified:

N/A

NERC Identified Issue:

What is the definition of "Annual", and how do registered entities implement that definition?

Proposed Effective Date: April 19, 2011

EEI Comments: EEI submits that NERC should not make arbitrary determinations of compliance when no clear definition of "Annual" exists. Although EEI broadly agrees that entities that define and follow their own internal definition of Annual are generally demonstrating best practices, we fear that this approach may also have the potential of unintentionally creating issues of possible non-compliance whenever a reliability standard specifically defines Annual and that definition conflicts with the definition used by the entity.

Therefore, EEI recommends that an entity who performed an annual requirement at an interval that generally meets any reasonable definition of "Annual", where no specific definition is provided in the standard, should be found in compliance of that requirement since the NERC Glossary of Terms does not currently define the term. As an alternative to the proposed language, EEI recommends that CAN-0010 be rewritten to state the following:

In lieu of a clear and specific definition of "Annual" contained or provided within a Reliability Standard, an entity who demonstrates that a Reliability Standard

Requirement was performed within a calendar year as required; or on a rolling 12 month basis; or within a period which could be reasonably considered as meeting the requirement of “Annual” should be considered as having met the minimum conditions of compliance. Therefore, CEAs are instructed not to find a potential non-compliance with a Reliability Standard Requirement if a registered entity has not developed a definition for Annual.

CAN-0011

Reliability Standard Referenced:

PRC-005-1

Reliability Standard Title(s):

Transmission and Generation Protection System Maintenance and Testing

Requirement(s) Identified:

R2

NERC Identified Issue:

Should CEAs review evidence of the pre-operational testing of a registered entity’s protection system equipment in connection with PRC-005 issues?

Proposed Effective Date: April 19, 2011

EI Comments: EEI is concerned that NERC, with the issuance of both CAN-0008 and CAN-0011, has begun a troublesome precedent of adding unnecessary levels of compliance complexity and risk through this duplicative compliance guidance. Specifically, both CAN-0008 and 0011 address the exact same standard, standard requirement and very similar compliance concerns. Requirement R2 obligates TOs and Distribution Providers who own transmission protection systems to provide maintenance and test programs and records to Regional Entities upon request. In CAN-0008, NERC asked the question: under what circumstances are CEAs required to consider evidence dated before June 18, 2007 while CAN-0011 asks should CEAs review evidence of pre-operational testing? To both questions EEI again submits the following:

“NERC Staff fully understands that prior to the date of enforcement there were no mandatory testing and maintenance cycles in place or required. Individual companies were allowed to test and maintain their equipment and systems per their own individual company procedures and policies. The standards were not developed to cast judgment on internal company procedures, policies or practices prior to the June 18, 2007 date. Additionally, there was no mandatory oversight or enforcement obligation prior to this date.”

Additionally, EEI believes that CEAs have a right to request test records, which could be used to document and verify equipment was tested prior to being placed in service, as long as the request does not include asking for records which extend to dates prior to the date of enforcement. (i.e., June 18, 2007). Therefore, we again submit that the compliance guidance should be:

CEAs are prohibited from requesting and engaging in enforcement of NERC Standards prior to June 18, 2007, which is the date the Commission legally approved the first

group of Reliability Standards. For that reason, Auditors are cautioned to restrict data requested to those periods as set by that date and moving forward. To do otherwise, would be a violation of the law. Any discovery of entity non-compliance prior to the date of enforcement cannot be used as justification for any enforcement action because the Standard was not enforceable prior to June 18, 2007.

Relative to newly installed equipment, specifically devices installed after the June 18, 2007 enforcement date, EEI does not agree that the “date the test was conducted is the appropriate date that should be used as the start date for the equipment’s maintenance and testing interval.” Instead, EEI believes that the plain language of the Standard should be used to assess compliance. To that point, we direct NERC to Requirement R1 which is the basis of an Entity’s testing interval:

R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:

R1.1. Maintenance and testing intervals and their basis.

R1.2. Summary of maintenance and testing procedures.

As plainly stated, it is the entity who determines testing intervals along with their basis, not the ERO. Therefore, we submit that the entity’s documented maintenance program would be the determining factor as to whether the maintenance cycle would begin from the point of commissioning or back to the pre-operational testing. However, in the event the entity’s maintenance and testing program does not provide a documented answer, that entity’s past practice should be sufficient. In either case, we see no reliability or compliance issue if an entity exercises either approach.

EEI further submits that new equipment testing is often conducted well in advance of placing the equipment in service. Unlike routine testing, new equipment is not subjected to real operating conditions and remains idle until it is placed in service. Therefore, we see no reliability risk to setting maintenance cycles based on the date the equipment was placed in service and feel the proposed compliance direction is arbitrary and without merit.

We therefore request that NERC reconsider the compliance direction provided in this CAN, integrate the compliance guidance provided in CAN-0008 and 0011 into a single document while allowing entities to develop maintenance cycles of new equipment based on their in-service date rather than any pre-operational testing.

CAN-0012

Reliability Standard Referenced:

N/A

Reliability Standard Title(s):

N/A

Requirement(s) Identified:

N/A

NERC Identified Issue:

Under what circumstances should a CEA verify completion of a periodic action or event during the implementation plan of a standard?

Proposed Effective Date: July 19, 2011

EI Comments: EEI disagrees with the compliance guidance provided within this CAN which supports the notion of “Bookends”. Although EEI generally agrees that conducting an initial test or assessment of a requirement on or prior to the date of enforcement is certainly a best practice. However, only if the Standard specifically requires such a test can issues of potential non-compliance be considered. Furthermore, entities are only obligated to comply with the written requirements of Reliability Standards and should not be held accountable for unwritten or implied requirements as defined by NERC or the Regions.

EEI submits that enforcement for any requirement begins on the day the standard becomes effective. Similarly, any obligation or demonstration of compliance prior to the date of enforcement would be similar to retroactive enforcement that is barred by ex post facto law. EEI believes that entities should only be judged on their compliance based on the plain language of the Standard and only from the point the standard becomes effective.

CAN-0013

Reliability Standard Referenced:

PRC-023 (*Version not specified*)

Reliability Standard Title(s):

Transmission Relay Loadability

Requirement(s) Identified:

R1 and R2

NERC Identified Issue:

What are the Effective Dates for switch-on-to-fault (SOTF) schemes?

Proposed Effective Date: June 17, 2011.

EI Comments: In general, EEI supports this proposed CAN. However, we recommend that the deletion of the reliability standard version as edited in this version of the CAN be restored or extended to include Version 2 if appropriate. As stated in our General Comments, we do not support “open ended” CANs.

CAN-0015

Reliability Standard Referenced:

Not identified in the Title

Reliability Standard Title(s):

Not identified in the Title

Requirement(s) Identified:

Not identified in the Title

NERC Identified Issue:

What are the performance obligations for a registered entity when a NERC Software Tool is unavailable?

Proposed Effective Date: July 19, 2011

EI Comments: EEI believes that CAN-0015 did not adequately address or provide necessary compliance direction. We strongly disagree with the use of footnotes as a means of providing compliance guidance such as can be seen in footnotes 5 and 7. As mentioned in our general comments, compliance guidance should be clear, concise, and to the point. We therefore ask that NERC avoid embedding compliance direction in footnotes of these documents.

As a primary method of providing clear compliance guidance and as the owner of these software tools, EEI believes that NERC should at a minimum within the body of this CAN identify all available NERC Software Tools, their specific use and whether alternate software solutions exist. Additionally, for those situations where no other software tool is available, NERC should provide some level of compliance direction that defines whether a manual process is required.

EEI does not believe that the compliance direction provided in example 2 would be effective if implemented as proposed. Here is an example. The proposed CAN states as follows:

2. During the time a NERC Software Tool is not available and a NERC Reliability Standard:
 - a. does not require the use of a NERC Software Tool, but
 - b. a NERC Software Tool is the only way to accomplish the requirement

And the compliance direction for this example as provided in the CAN:

In this situation, a CEA is not to verify whether a registered entity has an alternate method or back-up tool. However, a CEA is to verify evidence that the registered entity took necessary actions to act in the best interest of the interconnection at all times and accomplished the requirements of the standard at issue.

EEI believes that the compliance direction provided is not measureable and therefore unenforceable. EEI further submits that if a task can only be accomplished through the use of a single software tool and no reasonable manual process is available then no enforcement action can or should be considered. Furthermore, any suggestion that a CEA is to verify an entity "took necessary actions to act in the best interest of the interconnection at all times and accomplished the requirements of the standard at issue" is un-comprehensible since the example states that the "NERC Software Tool is the only way to accomplish the requirement".

Therefore, EEI recommends that NERC should either obligate entities to have an alternate method to accomplish compliance obligations, regardless of whether a software tool is available at any given time, or acknowledge that compliance with the standard without the use of the software tool is not possible. In either case, we believe the CAN needs substantial rework.

CAN-0022

Reliability Standard Referenced:

VAR-002-1.1b

Reliability Standard Title(s):

Generator Operation for Maintaining Network Voltage Schedules

Requirement(s) Identified:

R1 and R3

NERC Identified Issue:

May generators be operated in manual mode during start-up?

Proposed Effective Date: June 17, 2011

EEI Comments: EEI generally supports the compliance direction provided in this proposed CAN to be acceptable, however, we suggest that NERC should not provide “guidance regarding the start-up of generators” for any purpose. We believe NERC CANs should only provide compliance guidance relative to the Reliability Standards referenced not guidance on any operational task as is inferred. We recommend the following language:

For purposes of aiding a CEA, the CEA is to ensure any GOP who intends to “start-up” a generator in “Manual Mode” on either a one-time or routine basis has a documented protocol in place to meet the notification requirements as specified in VAR-002-1.1b.

Additionally, EEI recommends that under the section titled “Evidence of Compliance” the following be added:

The CEA are to assess that the entity has evidence they have a “Manual Start-up” notification protocol, followed the protocol requirements and maintained necessary document to verify their compliance.

CAN-0024

Reliability Standard Referenced:

CIP-002 – CIP-009 (*Version not specified*)

Reliability Standard Title(s):

Various

Requirement(s) Identified:

R3

NERC Identified Issue:

Can data diodes’ communication characteristics allow a cyber asset to be excluded from NERC Critical Infrastructure Protection (CIP) Standards?

Proposed Effective Date: Effective upon Posting

EI Comments: EI disagrees with the proposed CAN-0024. Although the proposed CAN appropriately frames an important question, the advice provided does not conform to the language of the Standard and ultimately expands the requirements of that standard beyond what had been written into Standard.

Specifically, CAN-0024 states that:

“the relevant criteria for determining whether non-critical CAs are to be classified as CCAs is the use of routable protocol to communicate outside the Electronic Security Perimeter.”

The CAN goes on to state:

“The use of a routable protocol to communicate to Cyber Assets outside the ESP will subject these assets to CIP Standards as CCAs.”

However the plan language of CIP-002-3 Requirement R3 states:

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 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.

EI submits that the plain language of CIP-002-3 clearly states that Critical Cyber Assets must always be “**essential to the operation** of the Critical Asset.” The second essential but not sole criterion is that communications must also exist, specifically, routable protocols that communicate outside the ESP, or routable protocols within a control center or dial-up accessible to that essential cyber asset. If a device does not meet **both** essential criteria it is not a CCA per the plain language of the Standard, but would be identified as a non-critical cyber asset and afforded the protections identified in CIP-005-3.

Additionally, EI questions why NERC feels compelled to direct CEAs to verify whether registered entities properly identified their CCAs as part of this proposed CAN, since the identified Issue is specific to the use of Data Diode devices and not the qualification of all cyber

assets. EEI also believes that CANs should not be a forum for educating the industry on topics such as “Data Diode” devices. We believe that those entities who have deployed or considered the deployment of such devices understand their functional operation. For those who do not have the requisite knowledge, NERC should use other tools to communicate these technical issues and not through the CAN process. Finally, we believe that NERC should not direct companies toward specific technical solutions necessary to meet the various requirements of Reliability Standards. We believe this type of compliance direction goes beyond the spirit of the Standards as written.

Finally, EEI recommends change in the compliance direction provided under “**Providing Evidence of Compliance**” (second Bullet) to read as follows:

- If a Cyber Asset was deemed not to be a CCA, the CEA should verify whether :
 - The CA was identified as “Not Essential to Operations” and listed as a Non-Critical Cyber Asset, or
 - Did not utilize routable protocols to communicate to Cyber Assets outside the ESP, or
 - Did not use a routable protocol within a control center; or
 - Was not dial-up accessible.

CAN-0026

Reliability Standard Referenced:

TOP-006 (*Version not specified*)

Reliability Standard Title(s):

Monitoring System Conditions

Requirement(s) Identified:

R3

NERC Identified Issue:

What is the scope of “protective relays” under TOP-006 R3?

Proposed Effective Date: June 17, 2011

EEI Comments: EEI believes that CAN-0026 has inadequately provided compliance direction for TOP-006, Requirement R3. The purpose of CANs as stated in the NERC CANs Process is to provide consistency in application and transparency in enforcement. Unfortunately, we view the compliance direction as provided in this CAN to be vague and lacking adequate compliance direction.

Under the section titled **Compliance Application**, NERC states:

CEAs are to verify that each RC, TOP and BA has provided to its operating personnel the relevant characteristics (including the purpose and limitations) of:

1. the protective relays that are applied in the applicable entity’s area, and

2. the protective relays, regardless of whether another entity has ownership or maintenance responsibility, that may impact that entity (the RC, TOP or BA).

First, EEI believes that it was not the intent of the standard to have system operators fully knowledgeable on the full body of protective relays that are used in an applicable entity's area. Instead, operators need to be knowledgeable of the basic operation of protective relays, aware of special protection schemes, as well as any limitations that may be in place on a transmission owner's network which might have the potential of adversely impacting the reliable operation of the grid.

EEI further recommends that appropriate compliance direction would have been to clarify what "appropriate technical information concerning protective relays" means. A clearer answer would have been to provide RCs, TOPs and BAs with specific examples, rather than simply stating they needed to provide "operating personnel the relevant characteristics (including the purpose and limitations)" for protective relays in their region. EEI submits that this CAN as written is vague and lacks necessary compliance direction. EEI recommends that CAN -0026 be revised to provide necessary compliance direction that is clear, concise, and to the point.

CAN-0028

Reliability Standard Referenced:

TOP-006 (*Version not specified*)

Reliability Standard Title(s):

Monitoring System Conditions

Requirement(s) Identified:

R1.2

NERC Identified Issue:

What are the resource responsibilities for BAs and TOPs under TOP-006?

Proposed Effective Date: July 19, 2011

EEI Comments: EEI recommends that CAN-0028 represents an example of where NERC demonstrated a lack of necessary discernment as to when a CAN is required. Specifically, EEI believes that the plain language of TOP-006, Requirement R1.2 is sufficiently clear as written. To that point we submit the plain language of R1.2:

Each Transmission Operator and Balancing Authority shall inform the Reliability Coordinator and other affected Balancing authorities and Transmission Operators of all generation and transmission resources available for use.

To our point, we believe there is no lack of understanding or awareness by companies on the resource responsibilities of BAs and TOPs. Therefore, providing compliance direction for something that is so completely understood and is so fundamental seems frivolous. Consequently, we recommend that CAN-0028 be withdrawn.

CAN Comment Form

Compliance Application Notice – 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Mike Garton
Phone Number: 804-819-2336
Email Address: mike.garton@dom.com
Entity Represented: Dominion – Multiple Entities
Region: SERC, RFC, NPCC, MRO

Primary Interest Groups

Are you suggesting a change to the groups mentioned? Yes / **No**

If yes, explain what change and why:

Issue

Are you suggesting a change to the issue statement of the CAN? Yes / **No**

If yes, explain what change and why:

CAN Summary

Are you suggesting a change to the CAN Summary? **Yes** / No

If yes, explain what change and why:

The language of the summary is too broad in its current state and does not properly restrict instructions to CEAs. The summary should be reworded to instruct CEAs to “find that data diodes that use routable protocols to communicate outside the ESP boundary cannot be used to exclude assets from compliance with CIP standards as CCAs.” Emphasis added to underlined section.

The sending or receiving hardware components of a data diode may include IP addressable hardware components in addition to hardware designed to transmit data from the sending component to the receiving component of the data diode. The existence of IP addresses and IP addressable cards alone is irrelevant to the application of CIP-002-3-R3.1. Ultimately, what’s relevant to CIP-002-3-R3.1 is the protocol that’s used to transport the data across the ESP boundary and how that transport mechanism is configured, not the protocol(s) used to move the data to the ESP boundary inside the ESP.

Background

Are you suggesting a change to the background statement of the CAN? **Yes** / No

If yes, explain what change and why:

1. The third paragraph of the background section is incorrect in its entirety and should be removed. The third paragraph states, ***“An easy way to assess this is to determine if any of the network interfaces on the stand-alone data diode device are configured with IP addresses. If the stand-alone data diode device has an IP address, it is “using” a routable protocol.”***

What’s relevant to CIP-002-3-R3.1 is the protocol that’s used to transport the data across the ESP boundary, not the protocol(s) that are used to move the data to the ESP boundary inside the ESP. Therefore, the determination of the use of a routable protocol isn’t as “easy” as is characterized above. Ultimately, CEAs need to review the relevant sections of the manufacturer’s design specification and the options used in the implementation of a data diode to determine whether or not a routable protocol is being used to transport data across the ESP boundary. If the communication between the sending and receiving components of the data diode does not use a routable protocol and the data diode is the only mechanism by which information is moved outside of the ESP, then the devices within the ESP do not use a routable protocol to communicate outside the ESP.

Additionally, the fact that a data diode has an IP address doesn’t mean that a routable protocol being used to send the data across the ESP boundary. As noted in the draft CAN, ***IP connectivity is assumed to be implemented primarily to minimize the impact to the “internal” Cyber Assets (inside the ESP).***

Dominion has identified two sample data diode implementations that should be characterized as using a routable protocol:

- 1) The data diode acts as a TCP/IP proxy when sending data across the ESP boundary
- 2) The data diode ‘wraps’ a routable protocol within the payload data sent across the ESP boundary.

In these sample implementations, Dominion believes sensitive information could theoretically be gleaned about cyber assets inside an ESP on the unprotected side of the network. In these implementations, Dominion suggest a conservative treatment of the data diode and considers the communications pathway across the ESP to use a routable protocol. In these cases, CIP-002-3 R3.1 is applicable.

2. The fourth paragraph of the background section makes a distinction between stand-alone and embedded data diodes. This distinction adds no value as Dominion is recommending the removal of the stand-alone device language in the Compliance Application Section and the embedded data

diodes aren't referenced outside of this section. The following paragraph is the fourth paragraph and should be removed: ***“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 purposes of this CAN, these will be referred to as “embedded data diode devices” to distinguish them from stand-alone data diode devices.”***

Compliance Application

Are you suggesting a change to the compliance application section of the CAN? Yes / No

If yes, explain what change and why:

The language of the last paragraph of the Compliance Application section implies that individual stand-alone sending and receiving components of a data diode that use a routable protocol to communicate solely on their respective sides of an ESP should be considered to use a routable protocol and does not appropriately clarify that the only relevant protocol is the one used to send data across the ESP boundary. If the communication between the sending and receiving components of the data diode does not use a routable protocol and the data diode is the only mechanism by which information is moved outside of the ESP, then the devices within the ESP do not use a routable protocol to communicate outside the ESP.

The sending or receiving hardware components of a data diode may include IP addressable hardware components in addition to hardware designed to transmit data from the sending component to the receiving component of the data diode. The existence of IP addresses and IP addressable cards alone is irrelevant to the application of CIP-002-3-R3.1. Ultimately, what's relevant to CIP-002-3-R3.1 is the protocol that's used to transport the data across the ESP boundary and how that transport mechanism is configured, not the protocol(s) used to move the data to the ESP boundary inside the ESP.

Dominion recommends the last paragraph of the Compliance Application section be simplified as follows: **“Therefore, under the current subrequirement of R3.1, the relevant criteria for determining whether non-critical CAs are to be classified as CCAs is the use of a routable protocol to communicate outside the Electronic Security Perimeter. 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

Are you suggesting a change to the effective period of the CAN? Yes / No

If yes, explain what change and why:

Evidence of Compliance

Are you suggesting a change to the evidence of compliance mentioned in the CAN? Yes / No

If yes, explain what change and why:

CAN Comment Form Compliance Application Notice – 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Todd Williams

Phone Number: 515-242-4384

Email Address: trwilliams@midamerican.com

Entity Represented: MidAmerican Energy Company

Region: MRO

Primary Interest Groups

Are you suggesting a change to the groups mentioned? Yes / No

If yes, explain what change and why:

No.

Issue

Are you suggesting a change to the issue statement of the CAN? Yes / No

If yes, explain what change and why:

Yes

MidAmerican Energy Company appreciates the opportunity to provide comments for Draft CAN-0024 (CIP-002 through CIP-009 Routable Protocols and Data Diodes) published on Monday, October 10, 2011. MidAmerican values NERC guidance and clarification with regard to the appropriate identification of Critical Cyber Assets but believes the Compliance Application Notice process tends to unnecessarily expand the NERC requirements.

It does concern MidAmerican that CAN's are being used to go beyond the standards and regulate minute details of how an entity maintains compliance with CIP standards.

In addition, MidAmerican supports the comments submitted by the Edison Electric Institute (EEI). Many of the points outlined in EEI's comments are reflective of MidAmerican's position on Draft CAN-0024.

Background

Are you suggesting a change to the background statement of the CAN? Yes / No

If yes, explain what change and why:

Yes, see comments above.

Compliance Application

Are you suggesting a change to the compliance application section of the CAN? Yes / No

If yes, explain what change and why:

Yes, see comments above.

Effective Period for CAN

Are you suggesting a change to the effective period of the CAN? Yes / No

If yes, explain what change and why:

Yes, see comments above.

Evidence of Compliance

Are you suggesting a change to the evidence of compliance mentioned in the CAN? Yes / No

If yes, explain what change and why:

Yes, see comments above.

CAN Comment Form Compliance Application Notice – 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Chris Parr

Phone Number: (816) 654-1372

Email Address: chris.parr@kcpl.com

Entity Represented: Kansas City Power & Light, KCPL - Greater Missouri Operations

Region: SPP

Primary Interest Groups

Are you suggesting a change to the groups mentioned? Yes / **No**

If yes, explain what change and why:

Issue

Are you suggesting a change to the issue statement of the CAN? **Yes** / No

If yes, explain what change and why:

Kansas City Power & Light (KCP&L) has substantial concerns regarding the remarks in the draft Compliance Application Notice, CAN-0024. First, the guidance provided to the CEA's in the section "Providing Evidence of Compliance" is no different than the criteria established in the Standard CIP-002-3 regarding routable protocols. If the compliance guidance provides no additional clarity than what is already established in the Standard, the CAN is not necessary.

Second, use of a CAN as an educational mechanism regarding technology or to express doubts regarding the use of technology as CAN-0024 suggests is not an appropriate use of the CAN process. The regulatory process established to provide guidance for consistency in audit practices is not the place to dictate the use or non-use of technology at the disposal of Registered Entities.

Much of CAN-0024 is reiterating the same language, criteria and content of CIP-002-3 and provides no other substantial guidance within the framework of the CIP Standards. And since the other remarks in CAN-0024 are the opinions and concerns expressed by NERC, it is recommended this CAN be considered for removal.

Background

Are you suggesting a change to the background statement of the CAN? Yes / **No**
If yes, explain what change and why:

Compliance Application

Are you suggesting a change to the compliance application section of the CAN? **Yes / No**

If yes, explain what change and why:

Kansas City Power & Light (KCP&L) has substantial concerns regarding the remarks in the draft Compliance Application Notice, CAN-0024. First, the guidance provided to the CEA's in the section "Providing Evidence of Compliance" is no different than the criteria established in the Standard CIP-002-3 regarding routable protocols. If the compliance guidance provides no additional clarity than what is already established in the Standard, the CAN is not necessary.

Second, use of a CAN as an educational mechanism regarding technology or to express doubts regarding the use of technology as CAN-0024 suggests is not an appropriate use of the CAN process. The regulatory process established to provide guidance for consistency in audit practices is not the place to dictate the use or non-use of technology at the disposal of Registered Entities.

Much of CAN-0024 is reiterating the same language, criteria and content of CIP-002-3 and provides no other substantial guidance within the framework of the CIP Standards. And since the other remarks in CAN-0024 are the opinions and concerns expressed by NERC, it is recommended this CAN be considered for removal.

Effective Period for CAN

Are you suggesting a change to the effective period of the CAN? **Yes / No**

If yes, explain what change and why:

Evidence of Compliance

Are you suggesting a change to the evidence of compliance mentioned in the CAN? **Yes / No**

If yes, explain what change and why:

CAN Comment Form

CAN Number 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Michael Mertz

Phone Number: 505-241-0676

Email Address: michael.mertz@pnmresources.com

Entity (ies) Represented: Public Service Co. of New Mexico, Texas New Mexico Power

Region(s): WECC, TRE

Primary Interest Groups

Do you disagree with the groups mentioned? No

If yes, explain why:

Issue

Do you disagree with the issue statement of the CAN? Yes

If yes, explain why:

- 1. Compliance application notices should be limited to “how” to audit, not how to “interpret” in order to audit. This CAN expands the scope of the requirement, and represents an interpretation that did not follow the FERC approved standards development/interpretation development process. If an interpretation is necessary for a CEA it should follow the standards development process.**
- 2. The issue statement does not recognize that use of a routable protocol does not change a Cyber Asset status from non-critical to critical. The Cyber Asset must first be considered essential, AND must also meet one of the qualifying connectivity criteria. The issue statement language could be confusing to a CEA and lead to an expansion of scope.**
- 3. The issue statement suggests a cyber asset can simultaneously be considered non-critical and critical. Suggest removing the word non-critical:**

“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 Cyber Assets from consideration as Critical Cyber Assets (CCA) when a routable protocol is implemented.

Background

Do you disagree with the background statement of the CAN? Yes

If yes, explain why:

- 1. The background section once again incorrectly implies a “Cyber Asset associated with a Critical Asset must be designated a CCA if it uses a routable protocol”. This is an incorrect statement. Only Cyber Assets that are first considered essential (R3) to the Critical Asset AND meet the qualifying connectivity characteristics identified in CIP-002 R3.1-R3.3 are considered Critical Cyber Assets.**
- 2. The statement: "...the relevant criteria for determining whether non-critical CAs are to be classified as CCAs is the use of a routable protocol..." leads to a possible conflict where a cyber asset is simultaneously non-critical and critical. Suggest removing the word non-critical. “Criteria” is plural while “is” is singular. We suggest using the singular form. We note that the acronym CA is not defined here, but is commonly used to mean "Critical Asset" From the context, we believe the author meant it to mean "Cyber Asset," so we suggest spelling the words out:**

“Therefore, under the current subrequirement of R3.1, the relevant criterion for determining whether Cyber Assets are to be classified as CCAs is the use of a routable protocol to communicate outside the Electronic Security Perimeter.”

Compliance Application

Do you disagree with the compliance application section of the CAN? No

If yes, explain why:

Effective Period for CAN

Do you disagree with the effective period of the CAN? No

If yes, explain why:

Evidence of Compliance

Do you disagree with the evidence of compliance mentioned in the CAN? No

If yes, explain why:

Oncor Electric Delivery Company LLC (Oncor) submits the following comments relative to the proposed CAN -0024.

Oncor's Response:

Oncor respectfully submits that the advice provided does not conform to the language of the Standard and ultimately expands the requirements of that standard beyond what had been written into the Standard. Oncor respectfully submits that CANs should not be a forum for educating the industry on topics such as "Data Diode" devices. Oncor takes the position that NERC should not direct the Industry on specific technical solutions necessary to meet the various requirements of Reliability Standards. We believe this type of compliance direction goes beyond the spirit of the Standards as written.

Thank you
Darryl Curtis
Reliability Standards Compliance
Oncor Electric Delivery

CAN Comment Form Compliance Application Notice – 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Tony Eddleman

Phone Number: 402-845-5253

Email Address: teddle@nppd.com

Entity Represented: MRO NSRF represented by: Madison Gas and Electric Company, Alliant Energy, Western Area Power Administration, Great River Energy, Xcel Energy, Rochester Public Utilities, Basin Electric Power Cooperative, Lincoln Electric System, American transmission Company, Wisconsin Public Service, Omaha Public Power District, Minnkota Power Cooperative, Midwest ISO, Otter Tail Power Company, Muscatine Power and Water, Nebraska Public Power District

Region: MRO

Primary Interest Groups

Are you suggesting a change to the groups mentioned? No

If yes, explain what change and why:

Issue

Are you suggesting a change to the issue statement of the CAN? No

If yes, explain what change and why:

Background

Are you suggesting a change to the background statement of the CAN? No

If yes, explain what change and why:

Compliance Application

Are you suggesting a change to the compliance application section of the CAN? Yes

If yes, explain what change and why:

Page 2, paragraph 4 states (emphasis added):

“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.*”

NSRF believes this is a statement of opinion and an engineering design or operational decision best left to the entity.

Similar language can be found on Page 2, paragraph 5. Again, judgment should be left to the entity based on their specific use-case.

“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.”

Effective Period for CAN

Are you suggesting a change to the effective period of the CAN? **Yes**

If yes, explain what change and why: Obviously this is an issue for some entities – a 12 month implementation of this standard interpretation should be provided to allow affected entities sufficient time install a perimeter security device.

Evidence of Compliance

Are you suggesting a change to the evidence of compliance mentioned in the CAN? **No**

If yes, explain what change and why:

CAN Comment Form

Compliance Application Notice – 0024

Please complete the CAN Comment Form and email it to cancomments@nerc.net.

Commenter Information

Name: Andrew Ginter

Phone Number: 403-264-6002

Email Address: andrew.ginter@waterfall-security.com

Entity Represented: Waterfall Security Solutions

Region: WECC

Primary Interest Groups

Are you suggesting a change to the groups mentioned? Yes / No: **NO**

If yes, explain what change and why:

Issue

Are you suggesting a change to the issue statement of the CAN? Yes / No: **NO**

If yes, explain what change and why:

Background

Are you suggesting a change to the background statement of the CAN? Yes / No: **YES**

If yes, explain what change and why:

Paragraphs 2-4 of the background section are not sufficiently specific or comprehensive. Waterfall recommends modifying the paragraphs to explain diode and forwarding concepts in greater detail, such as in the following recommended wording. Recommended deletions are crossed out. Recommended additions are in red font.

Data diode devices provide a “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 is to determine if any of the network interfaces on the stand-alone data diode device are configured with IP addresses. If the stand-alone data diode device has an IP address, it is “using” a routable protocol.~~

One type of data diode device consists of a single network appliance with at least two conventional network interfaces. At least one interface is connected into an “internal” IP network which serves CCAs, and at least one other interface is connected into an “external” IP network. Internal to the device are mechanisms to ensure that information flows exclusively from the “internal” network interfaces to the “external” interfaces. For the purposes of this CAN, such devices are referred to as “stand-alone data diode devices.”

Another type of data diode device consists of network interface cards that are installed into existing Cyber Assets. ~~One network card is only able to send information from the Cyber Asset to a network, and the other is able only to receive. A pair of Cyber Assets equipped this way are then connected to each other, and to an “internal” IP network serving CCAs, as well as to an “external” IP network, thus facilitating the unidirectional movement of information from the “internal” network to the “external” network. , and which provide the same uni-directional communication as stand-alone data diode devices.~~ For purposes of this CAN, these ~~devices are~~ will be referred to as “embedded data diode devices.” ~~to distinguish them from stand-alone data diode devices.~~

There are a number of tests which can be applied to determine when data diodes "use" the routable IP protocol in the sense of CIP-002-3 R3.1. All of the following circumstances indicate the use of the routable IP protocol:

- A stand-alone data diode device has network interfaces which have IP addresses assigned.
- An embedded data diode device has IP addresses assigned to one or both of the unidirectional network interface cards.
- Any data diode device, with or without IP addresses assigned to its network interfaces, which forwards IP traffic between networks by any means, including but not limited to routing, bridging and tunnelling.

Forwarding IP traffic may not always be obvious upon first inspection of the data diode configuration, but becomes evident when a network tap and any common packet sniffer are used to inspect data passing through the data diode system. Evidence of IP traffic entering or leaving a stand-alone data diode, or evidence of IP traffic passing from one NIC to another across an embedded data diode is evidence of "use" of the routable IP protocol. Further, evidence of IP packets containing IP

addresses arriving at any type of data diode from inside the ESP, and then being retransmitted essentially unchanged at some time later time outside the ESP to the IP address in the original packet, indicates routable traffic being forwarded through the data diode system.

In addition, the last two paragraphs of the existing "Background" section make good points about disadvantages of using data diodes in some circumstances. However, nowhere in the document are the advantages of data diodes mentioned. Waterfall recommends that for a fair and balanced treatment, the last two paragraphs be modified as follows:

Data diodes are attractive alternatives to firewalls because the diode devices can provide stronger protections for the integrity and availability of protected networks than firewalls are able to provide. Data diodes, transmitting data from the CCA portion of the network through the ESP to the “outside” portion of the network in a write-only fashion, can provide protections of integrity and availability equivalent to the protections offered by complete network isolation.

However, data diodes are not appropriate for all circumstances where firewalls might be used. For example, since ~~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 **between a set of PLC's or other control devices and an external supervisory systems, such as SCADA systems**, will not allow data requests, control commands, communication status feedback or set points from ~~external supervisory systems such as~~ **those SCADA systems to be transmitted to the control devices.**

Compliance Application

Are you suggesting a change to the compliance application section of the CAN? Yes / No: **NO**
If yes, explain what change and why:

Effective Period for CAN

Are you suggesting a change to the effective period of the CAN? Yes / No: **NO**
If yes, explain what change and why:

Evidence of Compliance

Are you suggesting a change to the evidence of compliance mentioned in the CAN? Yes / No: ***NO***

If yes, explain what change and why: