

Consideration of Comments

Project 2021-03 CIP-002

Comments Received Summary

There were 31 sets of responses, including comments from approximately 97 different people from approximately 78 companies representing 10 of the Industry Segments.

All comments submitted can be reviewed in their original format on the [project page](#).

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Manager of Standards Information, [Nasheema Santos](#) (via email) or at (404) 290-6796.

Consideration of Comments

The Project 2021-03 Drafting Team (DT) would like to thank all of industry for their time and comments. Due to the similar nature of multiple comments received during the comment period, the DT has chosen to respond to comments in summary format as provided for by section 4.2 of the Standard Processes Manual.

CIP-002 Communications Protocol Converters

The DT received multiple comments that have been categorized into the major themes below:

- Commentors stated that CIP-002 was not the right standard to address the scope of the Standard Authorization Request (SAR) as the determination of whether a Cyber Asset is a Bulk Electric System (BES) Cyber Asset does not fall within CIP-002.
 - CIP-003 or CIP-005 were mentioned as standards that may be better suited for addressing the scope of the SAR.
 - Other mechanisms such as a review of the BES Asset definition, review of exclusion language, Technical Rationale updates, and/or the development of guidance documents were mentioned as alternatives.
- Commentors stated that the SAR was overly broad and lacked clarity for purposes of identifying the risks to reliability that the SAR would address.

Drafting Team Response

The DT recommends the NERC Standards Committee reject the CIP-002 Communications Protocol Converters SAR, given the technical request of the SAR not clearly defining the reliability risks to the BES and that the scope of work of the SAR does not meet the CIP-002, CIP-003, and CIP-005 requirements or purpose. The inclusion of the protocol converters is inconsistent with the provisions for what the CIP-002 purpose is designed to do. Similarly, CIP-003 and CIP-005 are predicated upon identification in CIP-002, and given that CIP-002 does not have criteria for identifying Cyber Assets, the DT determined that the scope of the SAR would not be appropriately addressed in CIP-003 or CIP-005.

Serial communications do not require an entity to establish an Electronic Security Perimeter (ESP) or Electronic Access Point (EAP). This is because serial connections and their cables do not use routable protocols. Hence, a serial connection traversing a substation or Control Center perimeter (electronic or physical) and then connecting to a protocol converter is not in scope for CIP-005 and CIP-003.

CIP-002 requires entities to “Identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.” More specifically, entities are required to implement a process to identify high and medium impact BES Cyber System (BCS) at each transmission or generation asset using Attachment 1 criteria. This is a risk-based process. CIP-002 does not require entities to consider Cyber Assets associated with communications networks and data communication links between discreet ESP (4.2.3.2). CIP-002 does not require entities to consider specific devices within their process.

The current CIP-002-5.1a language allows entities the flexibility to consider applicable systems and Cyber Assets and to then determine which are critical to the BES. Critical Cyber Systems and Cyber Assets become BCS and BES Cyber Assets. Therefore, there is nothing in the language that precludes an entity from identifying and categorizing a protocol converter as a BES Cyber Asset. Also, there is nothing in the language that requires an entity to categorize a protocol converter as a BES Cyber Asset. Indeed, an entity may identify *any* device within its process that the entity believes will have an adverse impact upon the BES.

Lastly, the technical parameters in the SAR are insufficient in identifying the reliability risks or to be considered for revision into any of the CIP Standards.

Background Information

The purpose of the CIP-002 Communications Protocol Converters SAR is to consider the risks posed to the BES and BCS from the implementation and operation of communication protocol converters utilized throughout many entities’ gas and electric transmission and generation locations. Specifically, this SAR is to consider revising the existing CIP-002 standards to consider protocol converters as BES Cyber Assets and to clarify such a categorization.

Communication protocol converters are also known as media converters and are used throughout many gas and electric transmission and generation locations. They are typically smaller form factor hardware devices with interfaces used to attach differing physical media cable types. For example, an entity may connect a legacy serial meter via an RS232 serial cable on one side of the converter to an Ethernet cable connected on the other side of the converter. Within the converter are chipsets and/or software which convert the signal type from one type (such as serial Modbus) to another type (such as Ethernet Modbus). This allows entities flexibility to use advanced features of the end point device - such as providing remote access or enabling more data capabilities from endpoint devices or connecting multiple device types. These devices are generally categorized as networking equipment because they convert communication types

from one form to another. Many are used to connect older legacy serial devices to more modern Ethernet communications.