

Comment Report

Project Name: 2021-03 CIP-002 | Communications Protocol Converters SAR
Comment Period Start Date: 3/2/2023
Comment Period End Date: 3/31/2023
Associated Ballots:

There were 31 sets of responses, including comments from approximately 97 different people from approximately 78 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope as described in the CIP-002 Communications Protocol Converters SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.
2. Provide any additional comments for the drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
MRO	Jou Yang	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Chris Bills	City of Independence, Power and Light Department	5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc. (RTO)	2	MRO
					Bryan Sherrow	Board of Public Utilities	1	MRO
					Terry Harbour	Berkshire Hathaway Energy - MidAmerican Energy Co.	1	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
Shonda McCain	Omaha Public Power District	6	MRO					

					George E Brown	Pattern Operators LP	5	MRO
					George Brown	Acciona Energy USA	5	MRO
					Jaimin Patel	Saskatchewan Power Cooperation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
					Jay Sethi	Manitoba Hydro	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	1,3,4,5,6		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC) Project 2021-03 CIP-002	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Elizabeth Davis	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Andrew Gallo	Electric Reliability Council of	2	Texas RE

						Texas, Inc.		
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Jim Howell, Jr.	Southern Company - Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Sheraz Majid	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Chantal Mazza	Hydro Quebec	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Dan Kopin	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC

John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Nicolas Turcotte	Hydro-Québec TransEnergie	1	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Glen Smith	Entergy Services	4	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC
Shivaz Chopra	New York Power Authority	6	NPCC
Vijay Puran	New York State	6	NPCC

					Department of Public Service			
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC

1. Do you agree with the proposed scope as described in the CIP-002 Communications Protocol Converters SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer No

Document Name

Comment

The MRO NSRF agrees with the direction to add additional clarity for communication protocol converters.

The MRO NSRF suggests the scope of the SAR should also include a review of the exclusion:

Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters

The wording of the exclusion is what has created ambiguity. The SDT may not modify CIP-002 but instead update the exclusion. One of the intents of the exclusion is to enable RE to use third party telecommunication companies, and exclude equipment used by these companies as they are not a RE. The type of equipment in use by a telecommunication company in order to provide a service is not always known.

The SAR should take in to account if multiple protocol converters are used. For example, a protocol converter may be used to convert an incoming serial connection to an IP-based protocol. However earlier on in the transmission, the incoming serial connection may have been converter to an IP-based protocol, then converted back to a serial protocol.

Related projects must also include "Project 2016-02 Modifications to CIP Standards" as the SDT is working on a revision to the same exclusion to support the use of "super ESP" where and ESP spans multiple PSP.

The type of protocol conversion should also be considered by the SAR. Some protocol converters exist that translate a serial protocol in to another serial protocol. Others will convert a serial protocol to an IP based protocol. These represent two different categories of devices based on their connectivity.

Likes 0

Dislikes 0

Response

Alan Kloster - Evergy - 1,3,5,6 - MRO

Answer No

Document Name

Comment

Evergy supports and incorporates the comments of the Edison Electric Institute (EEI) for question #1.

Likes 0

Dislikes 0

Response

Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer No

Document Name

Comment

MidAmerican strongly supports EEI comments.

Likes 0

Dislikes 0

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer No

Document Name

Comment

Manitoba Hydro suggests the scope of the SAR should also include a review of the exclusion:

Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters

The wording of the exclusion is what has created ambiguity. The SDT may not modify CIP-002 but instead update the exclusion. The scope of the SAR should therefore include all of the NERC CIP standards as this exclusion text is included in all standards CIP-002 to CIP-013. One of the intents of the exclusion is to enable RE to use third party telecommunication companies, and exclude equipment used by these companies as they are not a RE. The type of equipment in use by a telecommunication company in order to provide a service is not always known.

The SAR should take in to account if multiple protocol converters are used. For example, a protocol converter may be used to convert an incoming serial connection to an IP-based protocol. However earlier on in the transmission, the incoming serial connection may have been converter to an IP-based protocol, then converted back to a serial protocol.

Related projects must also include "Project 2016-02 Modifications to CIP Standards" as the SDT is working on a revision to the same exclusion to support the use of "super ESP" where and ESP spans multiple PSP.

The type of protocol conversion should also be considered by the SAR. Some protocol converters exist that translate a serial protocol in to another serial protocol. Others will convert a serial protocol to an IP based protocol. These represent two different categories of devices based on their connectivity.

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer No

Document Name

Comment

NST agrees that as currently written, CIP-002 exception 4.2.3.2 (“Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters”) does not address situations where BES Cyber Systems within an ESP communicate with remote BES Cyber Systems that are Low Impact or have only serial communication interfaces and, consequently, no ESP. However, NST strongly disagrees with the notion that the best, in fact only, way to address this gap is by making significant and highly prescriptive changes to CIP-002.

The statement, “...this project supports reliability by clarifying how these protocol converters should be categorized and if they are to reside within a defined Electronic Security Perimeter” is problematic in two respects. First, CIP-002 already requires Responsible Entities to evaluate whether Cyber Assets either “used by and located at” or “associated with” BES assets (Control Center, generation or transmission facility, etc.) meet the definition of a BES Cyber System. If protocol converters are, for example, “used by and located” at a TOP Control Center, the TOP is already obligated to determine whether (a) they are Cyber Assets (per the NERC Glossary definition) and, if so, (b) they are BES Cyber Assets. Second, the obligation to locate High or Medium Impact BES Cyber Systems that meet certain criteria within an Electronic Security Perimeter is the province of CIP-005, not CIP-002. A protocol converter that is identified as a High or Medium Impact BCS and connects to a network using a routable protocol is already addressed by CIP-005. No additional requirement language is needed.

NST is unclear about the intended purpose of the paragraph that reads, “Additionally, when the protocol converters are physically located within the Transmission Operator’s Control Center, or associated datacenter, and not at the Transmission Owners transmission facility, the Transmission Operator owns and manages the protocol converters as opposed to the Transmission Owner. Other situations may exist where protocol converters are part of a Wide Area Network not owned or managed by either Registered Entity. In such situations, there is not an associated Functional Entity type defined in Appendix 5B of the Rules of Procedure.” Do the SAR authors believe these possible circumstances represent problems that need to be addressed? If so, the SAR does not appear to offer any proposed solutions.

The SAR is, in NST’s opinion, self-contradictory. It suggests that protocol converters should perhaps be classified as BES Cyber Systems and located with ESPs. A few short sentences later, it expresses concern about the possible security implications of using serial communications lines to connect external devices to BES Cyber Systems and/or PCAs within ESPs, thereby bypassing ESP Electronic Access Points.

The SAR mentions “authentication breaks” as a potential new requirement for serial communication links between BES Cyber Systems at different facilities. Do the SAR authors believe there should be requirements for remote serial communications similar to those for CIP-005 Interactive Remote Access, namely, the serial equivalent of Intermediate Systems? If so, the “Industry Need” section needs to be rewritten (it says nothing about authentication) and the Standard to be revised should be CIP-005, not CIP-002.

NST is particularly concerned about the statement, “Consideration should also be given to other types of Cyber Assets used in the communication paths, such as routers and switches, along with ownership and management of the Cyber Assets as applicable to Functional Entity types defined in Appendix 5B of the Rules of Procedure.” What communication paths, and whose Cyber Assets? Some communication links between BES Cyber Systems and “outside” (of either an ESP or a BES facility) traverse and use Responsible Entity corporate network infrastructures, which of course include switches and routers. This has the security benefit of allowing ESP Electronic Access Points to be situated within their respective corporate networks, as opposed to being directly connected to the public Internet. Forcing Entities to classify all Entity-owned routers and switches in such communication links as BES Cyber Systems because the links don’t qualify for the exception in Section 4.2.3.2 could have the unintended consequence of leading to Internet-facing CIP-005 Electronic Access Points, or, worse, an expectation that Responsible Entities should be obligated by the CIP Standards to protect everything, everywhere, all at once.

NST suggests that instead of proposing disruptive and, in our opinion, unnecessary changes to CIP-002 requirements, the problem with the language in

Section 4.2.3.2 (which, we note, seems to have been dealt with reasonably well by industry for the six years and nearly nine months that have elapsed since CIP Version 5 became effective) would be better addressed by revising that section instead of the entire Standard. Language similar to the “outside the asset” qualifier in CIP-003-8 Attachment 1 Section 3.1 could be used to address networks and data communication links to and from BES assets containing Low Impact BES Cyber Systems or Medium Impact BES Cyber Systems that have no ESP.

Likes 0

Dislikes 0

Response

Alison MacKellar - Constellation - 5,6

Answer

No

Document Name

Comment

Constellation aligns comments in agreement with Exelon.

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Justin Kuehne - AEP - 3,5,6

Answer

No

Document Name

Comment

AEP appreciates the opportunity to provide comments on the SAR for this project. We do not agree with the proposed scope laid out in the SAR and do not believe CIP-002 standard language should be modified due to communications assets already being addressed within the Exemptions Section 4.2.3 of the standard. If modifications to the standard are required, they should be made within the exemptions section rather than within the standard language. Moreover, the concepts laid out in the Detailed Description section of the SAR are more closely tied to CIP-005 rather than the scope of CIP-002, further diminishing the need to modify the standard requirements.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	
Comment	
<p>Texas RE generally supports clarifications to the Reliability Standard language requirements. However, in the present circumstances, Texas RE believes the current Reliability Standard language is clear. Moreover, the question of whether communication protocol converters between a Control Center and a transmission facility meet the definition of a BES Cyber Asset is dependent on design, configuration, and usage. Accordingly, further revision of the A 4.2.3 exemption language may result in additional confusion.</p> <p>Texas RE recommends considering the following in response to the SAR:</p> <ul style="list-style-type: none"> • The determination of whether a Cyber Asset is a BES Cyber Asset does not fall within CIP-002. CIP-002 requires entities to identify BES Cyber Systems or assets that contain BES Cyber Systems. In contrast, the determination of whether a Cyber Asset is a BES Cyber Asset hinges on the definition of BES Cyber Asset. As such, any clarifying revisions regarding the scope of the BES Cyber Asset definition would need to occur in the definition itself. This definition in turn implicates other CIP Standards and those impacts should be considered. • Texas RE is concerned with this statement: <p>“Additionally, when the protocol converters are physically located within the Transmission Operator’s Control Center, or associated datacenter, and not at the Transmission Owner’s transmission facility, the Transmission Operator owns and manages the protocol converters as opposed to the Transmission Owner. Other situations may exist where protocol converters are part of a Wide Area Network not owned or managed by either Registered Entity. In such situations, there is not an associated Functional Entity type defined in Appendix 5B of the Rules of Procedure.”</p> <p>Even though a piece of equipment may reside in a certain location does not mean it is owned by that location’s owner. Additionally, this situation is not unique to protocol converters. If it is determined that Wide Area Network (WAN) equipment owned or managed by entities that are not Functional Entities under the NERC Rules of Procedure pose a risk to the reliable operation of the Bulk Electric System then this risk should be addressed in a manner that addresses WAN equipment in general, not a specific subset of WAN equipment.</p> <ul style="list-style-type: none"> • In this statement, “There are inconsistencies in interpretations and approaches in categorizing such protocol converters when the Transmission Owner considers the transmission facilities to not have External Routable Connectivity or an Electronic Security Perimeter”, Texas RE notes that the existence of, or lack of, External Routable Connectivity does not impact whether exemption 4.2.3.2 applies. This exemption applies to Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters, both when External Routable Connectivity exists and when it does not. • Texas RE respectfully disagrees with this statement: <p>“This is found in transmission facilities with medium impact Bulk Electric System (BES) Cyber Systems having only serial communications traversing the physical location or transmission facilities with low impact BES Cyber Systems having no applicability for an Electronic Security Perimeter as required by CIP-005 (medium and high impact only).”</p> <ul style="list-style-type: none"> • CIP-005 contains requirements that must be performed when medium or high impact BCS are located within an ESP, however CIP-005 does not determine if an ESP exists. The definition of ESP does not include BCS impact ratings as a scoping mechanism. If a low impact BCS is connected to a network via a routable protocol then the logical border surrounding that network meets the legal definition of Electronic Security Perimeter. 	
Likes	0
Dislikes	0
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer No

Document Name

Comment

CIPv5 is predicated on the “System” concept, a BES Cyber System that has a real-time response and applicable BES reliability operating services (BROS) to support the reliable operation of the Bulk Electric System. Protocol converters residing in an ESP are already protected as PCA / BCA. Protocol converters residing outside an ESP are part of the transport Exemption 4.2.3. Serial traffic terminating outside of the ESP must be converted and forwarded through an Electronic Access Point (EAP).

BPA feels that the addition of this SAR to Project 2021-03 would result in too many disparate topics under the scope of one project/one SDT.

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer No

Document Name

Comment

First, the scope is not clear. The written scope says only CIP-002. The SAR includes topics that are addressed CIP-003 and CIP-005. How big is this scope?

Second, the scope requires the reader to interpret. This scope should be explicit. The SAR wants clarification on CIP-002 exemption 4.2.3 but quotes 4.2.3.2. The other items in 4.2.3 do not appear to be in question. As written, this point is too broad. Next, the request’s reason appears to be based on CIP-005 R1 and CIP-003. However the reader needs to connect those points. The reason should be more explicit.

Third, project 2016-02 (Modifications to CIP Standards) SDT is addressing the underlying question. Project 2016-02 has a V5TAG question on Interactive Remote Access (IRA) which is related to External Routable Connectivity (ERC). That SDT proposed IRA/ERC language earlier that addresses concerns with protocol converters.

Fourth, the industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. Project 2021-03’s (this CIP-002 SAR) title includes “protocol converter,” the underlying question will impact IRA and ERC, so there appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the on-going 2016-02 project and the proposed 2021-03 projects, we recommend that 2016-02 completes before 2021-03 project proceeds.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	
Comment	
<p>First, the scope is not clear. The written scope says only CIP-002. The SAR includes topics that are addressed CIP-003 and CIP-005.</p> <p>Second, the scope requires the reader to interpret. This scope should be explicit. The SAR wants clarification on CIP-002 exemption 4.2.3 but quotes 4.2.3.2. The other items in 4.2.3 do not appear to be in question. As written, this point is too broad. Next, the request's reason appears to be based on CIP-005 R1 and CIP-003. However the reader needs to connect those points. The reason should be more explicit.</p> <p>Third, project 2016-02 (Modifications to CIP Standards) SDT is addressing the underlying question. Project 2016-02 has a V5TAG question on Interactive Remote Access (IRA) which is related to External Routable Connectivity (ERC). That SDT proposed IRA/ERC language earlier that addresses concerns with protocol converters.</p> <p>Fourth, the industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. Project 2021-03's (this CIP-002 SAR) title includes "protocol converter," the underlying question will impact IRA and ERC, so there appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the on-going 2016-02 project and the proposed 2021-03 projects, we recommend that 2016-02 completes before 2021-03 project proceeds.</p>	
Likes	0
Dislikes	0
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
<p>Duke Energy supports the intent of the CIP-002 Communications Protocol Converters SAR, but recommends that the scope of the SAR is refined to address the identified need. This would start with a wider examination of the risk that these devices pose in various use cases, which in particular should consider the limited ability for many these devices to be misused or impact reliability upon failure or degradation, and not address simply as a categorization issue. If examination demonstrates an unacceptable reliability risk, the general need would be to revise the standards to provide consistent direction across regions on how entities should assess and protect applicable protocol conversion, specifically system-to-system communications. Limiting the scope of the SAR to CIP-002 precludes the option to edit CIP-005 to consider revisions based on any identified level of risk presented by these devices. Considering a classification change is not the most effective starting point for addressing the identified need.</p>	
Likes	0
Dislikes	0
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	No

Document Name	
Comment	
<p>We disagree with the SAR because of the below reasons:</p> <ol style="list-style-type: none"> 1. In the scope, the described scenario (serial between medium to low) is permitted by the existing standards, even though the protocol converters are to be classified BCA. It is unclear if the intent is to add the serial connections into the CIP standards. Such concerns may be discussed in CIP-005/CIP-003 instead of CIP-002; 2. This SAR may overlap with an existing initiative from SDT where the definition of IRA is to be revised in order to address the security concerns over IRA. 	
Likes	0
Dislikes	0
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - NA - Not Applicable	
Answer	No
Document Name	
Comment	
<p>CenterPoint Energy Houston Electric, LLC (CEHE) does not agree with the proposed scope of the SAR and supports the comments as submitted by the Edison Electric Institute (EEI).</p>	
Likes	0
Dislikes	0
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
<p>EEI does not support this SAR. There may be more appropriate tools to address this concern. We do not support CIP-002 attempting to clarify for all entities how to treat protocol converters in all situations and implementations. CIP-002 should not be changed to define detailed implementation within a CIP system. EEI suggests potentially modifying the CIP-002 technical rationale or the creation of guidance (e.g., white paper, technical paper, or implementation guidance) for aiding entities with this issue.</p>	

Likes 0

Dislikes 0

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 1,3,6

Answer

No

Document Name

Comment

NextEra Energy is not in agreement with the SAR request as documented. NERC has multiple SDTs and the impact of CIP-002 extends into other standards. NEE recommends NERC consolidate all CIP-002 SARs and issues into a scope that can address all downstream standards impact.

Likes 0

Dislikes 0

Response

Brent Sessions - Western Area Power Administration - 3 - MRO,WECC

Answer

No

Document Name

Comment

- The proposed SAR as written is incomplete. There is not cost impact assessment completed, which be required according to the form.
- There is an interpretation request also in process (2022-INT-01) which should be answered prior to a SAR being proposed. Without an interpretation, clarification seems unlikely.
- In the “Industry Need” section 3rd paragraph, the statement about TOP vs. TO ownership of transmission facilities is over-generalized and only represents one arhictectural and ownership scenario. It is unclear how to put management and/or ownership of specific equipment into a functional registration context.
- In the statement on Page 2, “Industry Need” section, 4th paragraph, “...consideration to the threat of unavailability, degradation, or misuse to a connected BES Cyber System and the aggregation of serial system-to-system communications from substations to Control Center BES Cyber Systems.” “Aggregation” in this context is vague—how much is too much? CIP-002 R1 already considers control centers as being a higher risk than an individual facility. Additionally, protocol converters do not “aggreate” communication paths—they only convert one protocol to another. Again this SAR assumes very specific BCS and communications architecture.

Likes 0

Dislikes 0

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter

Answer

No

Document Name	
Comment	
<p>FirstEnergy is supportive of EEI comments which state:</p> <p>EEI does not support this SAR. There may be more appropriate tools to address this concern. We do not support CIP-002 attempting to clarify for all entities how to treat protocol converters in all situations and implementations. CIP-002 should not be changed to define detailed implementation within a CIP system. EEI suggests potentially modifying the CIP-002 technical rationale or the creation of guidance (e.g., white paper, technical paper, or implementation guidance) for aiding entities with this issue.</p>	
Likes	0
Dislikes	0
Response	
<p>TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF</p>	
Answer	No
Document Name	
Comment	
<p>Southern Indiana Gas and Electric Company d/b/a CenterPoint Energy Indiana South (SIGE) would like to thank the SAR Standards Drafting Team for the opportunity to provide feedback on Project 2021-03 – CIP-002 Communications Protocol Convertors. SIGE does not agree with the proposed scope of the SAR and supports the comments as submitted by the Edison Electric Institute (EEI).</p>	
Likes	0
Dislikes	0
Response	
<p>Marcus Bortman - APS - Arizona Public Service Co. - 1,3,5,6</p>	
Answer	No
Document Name	
Comment	
<p>AZPS agrees with EEI’s suggestion to modify the CIP-002 technical rationale or create guidance for aiding entities with this issue. Guidance created to clarify categorization of communications protocol converters should include consideration for non-BES protocol converter nodes which relay converted serial communications between Control Centers and transmission facilities.</p>	
Likes	0
Dislikes	0
Response	

Sean Erickson - Western Area Power Administration - 1,6

Answer No

Document Name

Comment

· The proposed SAR as written is incomplete.

- o There is not cost impact assessment completed, which be required according to the form.
- o There is an interpretation request also in process (2022-INT-01) which should be answered prior to a SAR being proposed. Without an interpretation, clarification seems unlikely.
- o In the “Industry Need” section 3rd paragraph, the statement about TOP vs. TO ownership of transmission facilities is over-generalized and only represents one arhictectural and ownership scenario. It is unclear how to put management and/or ownership of specific equipment into a functional registration context.

In the statement on Page 2, “Industry Need” section, 4th paragraph, “...consideration to the threat of unavailability, degradation, or misuse to a connected BES Cyber System and the aggregation of serial system-to-system communications from substations to Control Center BES Cyber Systems.” “Aggregation” in this context is vague—how much is too much? CIP-002 R1 already considers control centers as being a higher risk than an individual facility. Additionally, protocol converters do not “aggreate” communication paths—they only convert one protocol to another. Again this SAR assumes very specific BCS and communications architecture.

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) Project 2021-03 CIP-002

Answer No

Document Name

Comment

The ISO/RTO Council (IRC) Standards Review Committee (SRC) does not agree with the proposed scope of this SAR for the following reasons:

The proposed scope of this SAR is unclear, as the SAR references topics addressed by CIP-003 and CIP-005, therefore going beyond the stated objective of modifying CIP-002. Additionally, references to exemptions available under 4.2.3 throughout the SAR should be revised to reference subpart 4.2.3.2, since this is the only exemption that appears to be in question.

There is already an existing project 2016-02 (Modifications to CIP Standards) in progress that includes the V5TAG question on Interactive Remote Access (IRA) that is related to External Routable Connectivity (ERC). This project has already proposed IRA/ERC language that addresses concerns with protocol converters. As such, there will be significant overlap and possible contradiction in required CIP-002 changes between project 2016-02 and the proposed addition to project 2021-03. Additionally, exemption 4.2.3.2 exists in other CIP Reliability Standards, such as CIP-005, CIP-007, and CIP-010, and any clarifications regarding the applicability of exemption 4.2.3.2 should also consider the potential impacts on all Standards that contain exemption 4.2.3.2. Project 2016-02 is already addressing modifications to multiple CIP Reliability Standards and is therefore a more appropriate project

for this SAR than project 2021-03, which is addressing a narrower subset of CIP Standards.

For these reasons, the SRC believes that the more appropriate path for this SAR is to leverage the Implementation Guidance processes vehicle rather than the SAR process. In order to avoid duplication of effort, the SRC also recommends that project 2016-02 be completed before project 2021-03 addresses the content of this SAR, or that this SAR be processed under project 2016-02 instead of under project 2021-03.

Likes 0

Dislikes 0

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer

No

Document Name

Comment

ERCOT joins the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer

No

Document Name

Comment

We do not agree with this SAR for four reasons.

First, the scope is not clear. The written scope says only CIP-002. The SAR includes topics that are addressed in CIP-003 and CIP-005. How big is this scope?

Second, the scope requires the reader to interpret. This scope should be explicit. The SAR wants clarification on CIP-002 exemption 4.2.3 but quotes 4.2.3.2. The other items in 4.2.3 do not appear to be in question. As written, this point is too broad. Next, the request's reason appears to be based on CIP-005 R1 and CIP-003. However, the reader needs to connect those points. The reason should be more explicit.

Third, project 2016-02 (Modifications to CIP Standards) SDT is addressing the underlying question. Project 2016-02 has a V5TAG question on Interactive Remote Access (IRA) which is related to External Routable Connectivity (ERC). That SDT proposed IRA/ERC language earlier that addresses concerns with protocol converters.

Fourth, the industry is trying to resolve earlier issues from multiple SDTs while simultaneously updating CIP Standards. Project 2021-03's (this CIP-002 SAR) title includes "protocol converter," the underlying question will impact IRA and ERC, so there appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing 2016-02 project and the proposed 2021-03 projects, we recommend that

2016-02 completes before 2021-03 project proceeds.

Likes 0

Dislikes 0

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer

No

Document Name

Comment

Southern Company supports the EEI comments around this SAR and do not feel it is needed in this form.

Likes 0

Dislikes 0

Response

James Keele - Entergy - 1,3,6

Answer

Yes

Document Name

Comment

Entergy suggests the scope of the SAR should also include a review of the exclusion: Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

Likes 0

Dislikes 0

Response

Teresa Krabe - Lower Colorado River Authority - 1,5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

David Jendras Sr - Ameren - Ameren Services - 1,3,6

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 5,6

Answer

Document Name

Comment

Constellation aligns comments in agreement with Exelon Generation.

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3

Answer

Document Name

Comment

PNMR is not in favor of the CIP-002 SAR to address the classification of protocol converters. Although clarification of the CIP-002 exemption may be necessary to address cyber assets associate with data communication between and ESP and a non-ESP, we do not believe the the use of a SAR is necessary. Perhaps revisions to NERC Glossary of Terms or technical rationale are more appropriate means to provide guidance to industry. PNMR supports similar sentiment expressed in EEI comments.

Likes 0

Dislikes 0

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer

Document Name

Comment

No comments received from Standard Owner or Subject Matter Experts

Likes 0

Dislikes 0

Response

2. Provide any additional comments for the drafting team to consider, if desired.

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer

Document Name

Comment

Southern Company supports the EEI comments around this SAR and do not feel it is needed in this form.

Likes 0

Dislikes 0

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer

Document Name

Comment

No response received from Standard Owner or Subject Matter Experts

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer

Document Name

Comment

We agree that some points need clarification. Updating Standards seems extreme when other means are available. Means like Request For Interpretation.

We agree with the clarification on protocol converters, but more than the topic of serial-to-IP such as converter location (inside/outside ESP?), is the converter an External Access Point (EAP)? How to address serial over copper to serial over fiber in the same facility?

We agree with clarification on facilities with Medium and Low. Scenarios and/or use cases will help.

We recommend this "industry need" include Generation.

Likes 0

Dislikes 0

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer

Document Name

Comment

ERCOT joins the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) Project 2021-03 CIP-002

Answer

Document Name

Comment

The IRC SRC agrees that some points regarding protocol converters need clarification, which can be obtained through other means outside of the SAR process, such as through the Implementation Guidance processes.

Specifically, the SRC agrees that there needs to be clarification regarding implementation methods to meet compliance with protocol converters in the scenarios of serial over copper to serial over fiber connections.

The SRC also agrees that clarification of scenarios and use cases is needed regarding facilities with Medium and Low impact rated cyber assets.

The SRC recommends that the “industry need” portion of the SAR be expanded to include measures regarding Generation facilities, since the same or similar hardware architectures could also exist in those environments and to maintain consistency with other portions of the SAR.

Likes 0

Dislikes 0

Response

Sean Erickson - Western Area Power Administration - 1,6

Answer

Document Name

Comment

· The potential scope of the proposed language on Page 3, “Consideration should also be given to other types of Cyber Assets used in the communication paths, such as routers and switches, along with ownership and management of the Cyber Assets as applicable to Functional Entity types defined in Appendix 5B of the Rules of Procedure” massively widens the scope to include all communication devices within a communications network. A communications network should be approached as an untrusted cloud, which CIP-005 already does. Overall the scope of the proposed “clarifications” is not clear.

· In the “Detailed Description” section, 1st paragraph, the language proposes enforcing an “authentication break” (undefined term) in the context of “system-to-system serial communication protocol converters”. Given system-to-system communication is not considered Interactive User Access, the term “authentication break” does not have a relation to this use case—it is unclear whether the proposal is for *authorization* or for *authentication*. This issue is also addressed in the 2022-INT-01 interpretation request.

· It is unclear what reliability or security risks are being mitigated by moving a protocol converter inside an ESP. In the proposed language, an ESP would only provide protection on the routable protocol side of the protocol converter, and not on the serial side of the converter, thereby only protecting one direction of the communication (routable -> serial). Moving the protocol converter inside the ESP brings the serial network inside the ESP, which would not be protected (serial -> routable).

· CIP-002 also provides the opportunity to implement a process to assist in the identification of high or medium BCS. Therefore, further clarification is not needed. This leads directly back to the previous comment about if the protocol converter being considered as part of the communication system. If that protocol converter has to be in the scope of CIP-002, then all communications components need to be. Instead of a SAR leading to a “one size fits all” solution, how the protocol converters are identified and protected should be assessed on a case-by-case basis given the various architectural options possible, and given the Responsible Entities process(es) for identifying and mitigating risks.

Likes 0

Dislikes 0

Response

Marcus Bortman - APS - Arizona Public Service Co. - 1,3,5,6

Answer

Document Name

Comment

AZPS has no additional comments at this time.

Likes 0

Dislikes 0

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter

Answer

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

James Keele - Entergy - 1,3,6

Answer

Document Name

Comment

Clarification on protocol converters since some are non-programmable devices. How to handle dial up connections or legacy non-IP communications. The topic of serial-to-IP such as converter location (inside/outside ESP?), is the converter an External Access Point (EAP)? How to address serial over copper to serial over fiber in the same facility?

Likes 0

Dislikes 0

Response

Brent Sessions - Western Area Power Administration - 3 - MRO,WECC

Answer

Document Name

Comment

- The potential scope of the proposed language on Page 3, “Consideration should also be given to other types of Cyber Assets used in the communication paths, such as routers and switches, along with ownership and management of the Cyber Assets as applicable to Functional Entity types defined in Appendix 5B of the Rules of Procedure” massively widens the scope to include all communication devices within a communications network. A communications network should be approached as an untrusted cloud, which CIP-005 already does. Overall the scope of the proposed “clarifications” is not clear.
- In the “Detailed Description” section, 1st paragraph, the language proposes enforcing an “authentication break” (undefined term) in the context of “system-to-system serial communication protocol converters”. Given system-to-system communication is not considered Interactive User Access, the term “authentication break” does not have a relation to this use case—it is unclear whether the proposal is for *authorization* or for *authentication*. This issue is also addressed in the 2022-INT-01 interpretation request.
- It is unclear what reliability or security risks are being mitigated by moving a protocol converter inside an ESP. In the proposed language, an ESP would only provide protection on the routable protocol side of the protocol converter, and not on the serial side of the converter, thereby only protecting one direction of the communication (routable -> serial). Moving the protocol converter inside the ESP brings the serial network inside the ESP, which would not be protected (serial -> routable).
- CIP-002 also provides the opportunity to implement a process to assist in the identification of high or medium BCS. Therefore, further clarification is not needed. This leads directly back to the previous comment about if the protocol converter being considered as part or the communication system. If that protocol converter has to be in the scope of CIP-002, then all communications components need to be. Instead

of a SAR leading to a “one size fits all” solution, how the protocol converters are identified and protected should be assessed on a case-by-case basis given the various architectural options possible, and given the Responsible Entities process(es) for identifying and mitigating risks.

Likes 0

Dislikes 0

Response

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - NA - Not Applicable

Answer

Document Name

Comment

CEHE has no additional comments.

Likes 0

Dislikes 0

Response

Alain Mukama - Hydro One Networks, Inc. - 1,3

Answer

Document Name

Comment

Generally, we agree that clarification would be needed for the categorization of some protocol converters. However, instead of updating the standard, a different mean, such as guideline, may be used to provide clarification on them. Examples of protocol converters (including but not limited to serial-to-ip converter) and use cases would be very helpful.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer

Document Name

Comment

Given that Project 2021-03 already has three other SARs, and the potential complexity of addressing this topic, a stand alone project should be

considered. The potential CIP-005 implications of addressing this topic would be challenging to address in 2021-03.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Québec TransEnergie - 1

Answer

Document Name

Comment

We agree that some points need clarification. Updating Standards seems extreme when other means are available. Means like Request For Interpretation.

We agree with clarification on protocol converters, but more than the topic of serial-to-IP such as converter location (inside/outside ESP?), is the converter an External Access Point (EAP)? How to address serial over copper to serial over fiber in the same facility?

We agree with clarification on facilities with Medium and Low. Scenarios and/or use cases will help.

We recommend this "industry need" include Generation.

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Québec Production - 1,5

Answer

Document Name

Comment

We agree that some points need clarification. Updating Standards seems extreme when other means are available. Means like Request For Interpretation.

We agree with clarification on protocol converters, but more than the topic of serial-to-IP such as converter location (inside/outside ESP?), is the converter an External Access Point (EAP)? How to address serial over copper to serial over fiber in the same facility?

We agree with clarification on facilities with Medium and Low. Scenarios and/or use cases will help.

We recommend this "industry need" include Generation.

Likes 0

Dislikes 0

Response

Alison MacKellar - Constellation - 5,6

Answer

Document Name

Comment

Constellation aligns comments in agreement with Exelon.

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer

Document Name

Comment

Regarding the SAR form's last question ("Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives."), NST disagrees with the answer given ("None"). While it may be true that no alternatives have been considered, we believe that if industry needs help with determining if and how protocol converters used for routable/serial communications links between BES Cyber Systems at different BES assets should be subject to CIP Requirements, a well-written guideline document would be a significantly better and less disruptive solution than an attempt to rewrite CIP-002.

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 5,6

Answer

Document Name

Comment

Constellation aligns comments in agreement with Exelon Generation.

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Comments received from Kinte Whitehead/Exelon

1. Do you agree with the proposed scope as described in the CIP-002 Communications Protocol Converters SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

Yes

No

Comments: Exelon has elected to align with EEI in response to this question.

2. Provide any additional comments for the drafting team to consider, if desired.

Comments: