Comment Report

Project Name:	2023-04 Modifications to CIP-003 | SAR
Comment Period Start Date:	3/31/2023
Comment Period End Date:	5/15/2023
Associated Ballots:	

There were 37 sets of responses, including comments from approximately 112 different people from approximately 89 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 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 SAR 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
WEC Energy Group, Inc.	Christine Kane	3,4,5,6		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Tacoma Public Utilities (Tacoma, WA)	Jennie Wike	1,3,4,5,6	WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Ryan Strom	Buckeye Power, Inc.	5	RF
					kylee Kropp	Sunflower Electric Power Corporation	1	MRO
					Nikki Carson-Marquis	Minnkota Power Cooperative	NA - Not Applicable	MRO

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
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

Alain Mukama	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
Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	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
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 Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Joshua London	Eversource Energy	1	NPCC
Western Electricity Coordinating Council	Steven Rueckert	10		WECC	Steve Rueckert	WECC	10	WECC
					Phil O'Donnell	WECC	10	WECC

1. Do you agree with the proposed scope as described in the 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.

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC requests consideration of collapsing the low impact requirements with CIP-005 and CIP-007 instead of continuing to have a separate requirement within CIP-003 for low impact. If the requirements cannot be collapsed into those standards, ATC requests consideration that the defined ESP term does not extend to low impact; and, there is therefore no External Routable Connectivity applicable either. This SAR may need to introduce formally a L-ESP and L-ERC, which would also then possibly include Low-EACMS and Intermediate Systems. ATC also supports EEI and NSRF comments.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Tacoma Power does not agree with the proposed scope described in the SAR.

This SAR is proposing more strict controls for low impact BCS with ERC than the controls currently required in CIP-005 for medium impact BCS without ERC. By imposing more strict controls on low impact BCS with ERC, this is upending the CIP-002 categorization. The NERC Standards establish low/medium/high impacts in CIP-002 and fulfill Requirements based on this impact in the other CIP Standards. A low impact BCS should not have more controls than a medium impact BCS. This SAR is placing greater emphasis, and more restrictive controls, on lows with IP connectivity than medium impact BCS without ERC. This begs the question of whether medium BCS without ERC should now be classified as low impact, and lows with IP connectivity should be classified as medium impact. In summary, the amount of controls applied to a type of asset should be dependent on its categorization. Tacoma Power does not agree with creating a precedent for applying greater controls to low impact BCS.

Tacoma Power is also concerned that the scope of this SAR is broad, and as a result, will be difficult to implement. For example, the term “remote access” used in the Detailed Description section is not defined and depending on how an entity defines this term, it will impact the scope of the Requirement(s). The SAR should clarify whether “remote access” is referring to north-south or east-west communication.

Lastly, instead of focusing on asset-level detection, Tacoma Power recommends that the SAR should focus on defining and establishing an Electronic Security Perimeter (ESP) for low impact BCS, and then requiring detection/monitoring of malicious communication at the ESP boundary. This approach is easier to understand and implement than focusing on new Requirements based on asset-level detection. Tacoma Power recommends re-wording the third bullet in the Detailed Description section to the following:

“Requirement(s) for establishing an ESP for low impact BES Cyber Systems with external routable connectivity, and detecting malicious communications at the ESP boundary.” If the SAR drafting team keeps the approach for requiring asset-level detection, then Tacoma Power recommends changing the “to/between” language in the third bullet to “inbound and outbound” to align with the CIP-003-9 Section 6.3 language, as follows: “Requirement(s) for detection of **inbound and outbound malicious communications between assets** containing low impact BES Cyber Systems with external routable connectivity.”	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF does not support the proposed scope as described in the SAR. The narrative needs to be revised to state, “malicious communications to/between assets”. The “to/between” is missing in the current form of the SAR scope. The NAGF also requests clarification as to the context, objective, and measurability for “protection of user authentication information in transit.” There is ambiguity and confusion as to where protection responsibility extends outside of the Low Impact Facility. Lastly, the NAGF requests clarity on the term “malicious” and its definition relating to the scope of the types of communication to be detected between Low Impact BES Cyber Systems with ERC.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Regarding Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity, BPA suggests mimicking CIP-005 R2.2. Regarding Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity: this raises the bar of Low with ERC higher than Medium with ERC and creates misalignment in the standards. BPA suggests coordinating this change after changes to Medium ERC so utilities can address the greater risk first.	
Likes 0	

Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	No
Document Name	
Comment	
Constellation Aligns with the NAGF to vote in the negative to Question 1. Constellation agrees with comments from the NAGF and agrees with comments provided by Exelon and IEEE and does not agree with voting in the affirmative. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI and MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
PNMR does not agree with the scope as described in the SAR.	

While PNMR does agree that coordinated attacks present risk, it is unclear as to the realized risk associated with a coordinated attack utilizing multiple low-impact BES Cyber Systems. As it would be difficult to quantify the number of low-impact systems needed to be utilized in a potential coordinated attack and with uncertain findings as to the use of low-impact systems to conduct a coordinated attack, PNMR believes the potential risk to the BES from such attacks does not sufficiently correlate with the proposed authentication and detection controls which would be a vast expansion of scope.

The NERC Low Impact Criteria Review Report references the risk of coordinated attacks on low impact BES Cyber Systems for those systems that are determined by the CIP-002 Standards. However, the CIP-002 categorization of BES Cyber Systems is not intended to take into account the effect of a coordinated attack in determining the categorization of a BES Cyber System. This language seems to attempt to change the purpose and muddy the scope of the CIP-002 Standard.

PNMR also has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 5,6

Answer	No
Document Name	

Comment

Constellation Aligns with the NAGF to vote in the negative to Question 1. Constellation agrees with comments from the NAGF and agrees with comments provided by Exelon and IEEE and does not agree with voting in the affirmative.

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NST strongly suggests not using the phrase, "external routable connectivity" as a qualifier for identifying low impact assets containing BES Cyber Systems that would be subject to any proposed new requirements, notwithstanding the fact the LICRT report uses it. We likewise see no need to "create a new defined term or modify an existing defined term." We respectfully note that an earlier Standard Drafting Team's attempt to define a low impact version of External Routable Connectivity, "LERC," was abandoned for lack of industry support. It is our opinion that the SAR and new SDT can

and should use the existing language from CIP-003-8 Attachment 1 Section 3 Part 3.1 to identify low impact assets containing BES Cyber Systems that would be subject to any proposed new requirements.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The cost impact to modify the low impact criteria could potentially be significant. Depending on the encryption requirements for authentication, latency might be added to communication at remote sites.

The current wording in bullet points 2 and 3 of the scope suggests applying new, more rigorous and potentially very costly standards to Low Impact systems before applying to High and Medium Impact systems. This creates additional burden on Low Impact before addressing the risks within the higher impact systems. The intent and interpretation of the phrase “protection of user authentication information in transit for remote access”(e.g. encrypting username and password information in transit between low impact systems), could negatively impact reliability when encryption introduces latency in critical communications. Also, the proposed requirement “for detection of malicious communications to/between assets containing low impact BES Cyber Systems” could have conflicting or confusing requirements with upcoming regulation regarding "Internal Network Security Monitoring.”

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

While a coordinated cyber-attack on low impact BCS could be impactful to the BES, it would only be temporary. A coordinated physical attack would be more likely and have a significantly greater impact to the BES. Further ANY allowed electronic access to and from low impact BCS should be legitimate traffic per CIP-003 required Electronic Access Controls.

For easy numbers sake, let’s say 10% of all connected low impact BCS are controlled by low impact Control Centers and the low impact Control Centers are included in that 10%. That would mean 90% of all low impact BCS, that have ERC, already have required Electronic Access Controls. If the low impact controls fail, 90+% of low impact BCS are connected to a higher upstream (medium and high Control Centers at RC, BA, TOP, GOP) BCS which have required Electronic Access Points with stricter access controls and malicious communication detection required. The upstream BCS cyber security controls are in place to detect malicious communications.

Low impact BCS have requirements to detect malicious communication for vendor communications. Thus if a coordinated attack takes place, it would take significant resources unless backdoor/trojan was installed along the software supply chain making traffic appear legitimate, which in that case NO control would detect the nefarious connections, just as in the Solarwinds case. With different entities, using different manufacturers of Cyber Assets in their BCS, even with a distributed supply chain attack, the attack would have a relative small footprint unless the adversaires were able to attack supply chain at multiple vendors and execute a simultaneous attack. That likelihood is incredibly low.

A coordinated physical attack is more likely than a coordinated cyber-attack on low impact BCS. A coordinated planned physical attack on major transmission and generation assets would have a significantly greater impact on the US and last significantly longer than any cyber-attack. A coordinated physical attack would much easier to execute than coordinated cyber-attack on low impact BCS, if an adversary were trying to impact the reliability of the BES. If a coordinated attack on low impact BCS was executed, it should already be detected by existing controls.

Responding directly to the SAR: how would adding requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity reduce the risk of a coordinated attack? To remotely access a low impact BCS, it has to already be permitted by the entity's Electronic Access Controls. If traffic is not approved by the entity, it would be blocked per CIP-003 R2. Thus the access control already exists or an attacker has already bypassed all controls. Further, most attacks leverage vulnerabilities not usernames and passwords to bypass authentication completely.

A coordinated attack would have to come from within multiple entities, with enough combined low impact BCS to cause a BES reliability issue, which already have cybersecurity controls in place, as the traffic would have to be allowed or a well-planned distributed physical installation of nefarious Cyber Assets in a low impact BCS or distributed supply chain attack, or a distributed physical cyber-attack. In any case again these would be short lived attacks compared to a physical attack. If an adversary has to physically go to a location to attack it, physical damage is more than likely what is going to be done at a minimum. We are not suggesting the necessity of usernames and passwords is irrelevant, we are suggesting that this is already a best practice and don't need a new requirement due to the existing controls along with best practices.

There are already requirements to detect malicious Vendor communications. There still aren't requirements for medium impact BCS to have malicious communication detections. This has been brought a number of times.

From a SAR perspective on malicious communication detection, it could have been written this way when it was added to CIP-003 previously. The current proposed change in our opinion should be modified to detect all malicious communications entering or leaving a low impact BCS, not just detecting malicious communications from Vendor remote access, as it is now or as it's written in the SAR from low impact to low impact. Combining the requirement into a singular requirement covering the entire scope of BCS to BCS communications would make the requirement significantly easier to comply with. If we are going to require detections and look at this from a risk lense, we should be monitoring all traffic in and out of a low impact BCS, not just looking specifically where traffic is destined to or from ie low to low or vendor.

Considering the probability and impact, a coordinated cyber-attack on low impact BCS could possibly impact the reliability of the BES. But in this case, when considering risk and modifying requirements to close gaps, we should also consider the longevity of the impacts compared to other risks and prioritize. While a distributed cyber-attack on the BES could impact the reliability of the BES, the longevity of the impact would be much shorter than a physical attack even without sound backup plans.

With protections and controls already in place for low impact BCS, we don't feel adding more requirements to protect against a distributed cyber-attack on the BES will close any real gaps. The highest identified risks in the report are covered by existing controls.

If we are going add these controls to low impact BCS, what about potentially completely unprotected systems that an entity may have that are non BES which may also traverse the same networks? Are there going to be additional controls there? What about corporate systems that traverse the same networks, are we going to add controls there too to protect against a distributed attack, as low impact BCS are often in an enclave off corporate networks?

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	

The project scope includes the use of External Routable Connectivity in which the current definition requires the boundary of Electronic Security Perimeter which does not apply to Low Impact BES Cyber System. Further clarificiation in the socpe is required as it is unclear whether boundary is at outside of the network of Low Impact BES Cyber System or outside of the asset containing the Low Impact BES Cyber System.

It is unclear what "remote access" is included in the scope. Is it the user interactive access initiated from outside of the network of Low Impact BES System or outside of the asset containing Low Impact BES System(s)?

Likes 0	
Dislikes 0	
Response	

Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

AES Clean Energy supports the MRO NSRF's comments on this Unofficial Comment Form - see below.

"The MRO NSRF agrees with the intent of the proposed scope of the SAR. However, the security controls should be scoped as “to or from BES Cyber Systems that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset.” This language more appropriately scopes the types of devices that need to be in scope of the CIP-003 Standard and excludes Cyber Assets at a low-impact asset that are not scoped as BES (e.g., corporate communication). The MRO NSRF suggests the following language to be used in the SAR:

Project Scope (Define the parameters of the proposed project):

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications to or from BES Cyber Systems with external routable connectivity that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset.

Detailed Description:

Modify CIP-003-9 to add:

- Requirement(s) for authentication of remote users before access is granted to BES Cyber Systems with external routable connectivity that are located within low impact assets.
- Requirement(s) for protection of user authentication information in transit for remote access to or from low impact BES Cyber Systems with external routable connectivity located within low impact assets.
- Requirement(s) for detection of malicious communications sent to or from BES Cyber Systems with external routable connectivity that reside within low impact assets and Cyber Assets that exist outside the low impact cyber asset.

Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NSRF agrees with the intent of the proposed scope of the SAR. However, the security controls should be scoped as “to or from networks for BES Cyber Systems that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset.” This language more appropriately scopes the systems that need to be in scope of the CIP-003 Standard and excludes other types of systems at a low-impact asset that should not be in scope. (e.g., corporate communication). The MRO NSRF suggests the following language to be used in the SAR: Project Scope (Define the parameters of the proposed project): Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications on BES Cyber Systems networks that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset. Detailed Description: Modify CIP-003-9 to add:	

- Requirement(s) for authentication of remote users before access is granted to the networks of BES Cyber Systems that are located within low-impact assets.
- Requirement(s) for protection of user authentication information in transit for remote access to networks for low-impact BES Cyber Systems located within low-impact assets.
- Requirement(s) for detection of malicious communications sent on networks to or from BES Cyber Systems that reside within low-impact assets.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

MidAmerican agrees with the proposed scope, but urges NERC to make the clarifications requested in EEI and MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 1,3

Answer	Yes
Document Name	

Comment

Exelon is aligning with EEI's response to this question.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment
Southern Company agrees with the EEI comments.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment
CenterPoint Energy Houston Electric, LLC (CEHE) supports the intent of the proposed scope of the SAR. The proposed enhancements add controls to authenticate remote users and protect information in-transit; however, CEHE is concerned specifically with this bulleted item from the SAR, "*Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity*." This language needs to be clarified. CEHE supports the comments as submitted by the Edison Electric Institute (EEI) as it relates to the proposed language for the "Project Scope" of the SAR.

Likes 0	
Dislikes 0	

Response

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	

Comment
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 2023-04 – Modifications to CIP-003. SIGE agrees with the proposed scope of the SAR and supports the comments as submitted by the Edison Electric Institute (EEI) as it relates to the proposed language for the "Project Scope" of the SAR.

Likes 0	
Dislikes 0	

Response

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

Document Name	

Comment

Duke Energy agrees with the proposed scope and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the intent of the proposed scope of the SAR noting that it closely aligns with the findings of NERC's Low Impact Criteria Review Team (LICRT). While we support this SAR, there are issues that need to be clarified:

1. The LICRT recommendation is limited in scope to communications to and from BES Cyber Systems and while there may be other systems at those locations containing low impact BES Cyber Systems (e.g., corporate communications, etc.), these other assets and their communications should be considered as outside the scope of this SAR.
2. The term external routable connectivity (ERC), as included in the recommendations of this SAR, applies to communications as currently established according to CIP-003, Attachment 1, Section 3.1. Given the term is already defined for medium and high impact BES Cyber Systems, the meaning and how it relates to Low Impact Cyber systems and assets will likely result in confusion without a separate definition. We suggest the SDT define Low Impact ERC.
3. Lastly, the scope of the requirement for the detection of "malicious communications to or between assets containing low impact BES Cyber System with external routable connectivity" should be limited to the detection of external communications to and between facilities containing low impact BES Cyber Systems and not all internal communications within a facility network at a discrete location.

We also suggest that the Project Scope language be modified (bold text) as follows:

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications **to networks** containing low impact BES Cyber Systems **from Cyber Assets outside the assets, for those assets** with external routable connectivity.

Additionally, we suggest that the third bulleted recommendation contained in the Detailed Description section of the SAR include the following modification (bold text) to address our concern regarding the intended scope.

Requirement(s) for detection of malicious communications **sent to or from networks** containing low impact BES Cyber Systems **from Cyber Assets outside the asset, at assets** with external routable connectivity.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
WEC Energy Group supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 1,3,6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy agrees with EEI's comments which state: EEI supports the intent of the proposed scope of the SAR noting that it closely aligns with the findings of NERC's Low Impact Criteria Review Team (LICRT). While we support this SAR, there are issues that need to be clarified: 1. The LICRT recommendation is limited in scope to communications to and from BES cyber systems and while there may be other systems at those locations containing low impact BES Cyber Systems (e.g., corporate communications, etc.), these other assets and their communications should be considered as outside the scope of this SAR.	

2. The term external routable connectivity (ERC), as included in the recommendations of this SAR, applies to communications as currently established according to CIP-003, Attachment 1, Section 3.1. Given the term is already defined for medium and high impact BES Cyber Systems, the meaning and how

it relates to Low Impact Cyber systems and assets will likely result in confusion without a separate definition. We suggest the SDT define Low Impact ERC.

3. Lastly, the scope of the requirement for the detection of "malicious communications to or between assets containing low impact BES Cyber System with external routable connectivity" should be limited to the detection of external communications to and between facilities containing low impact BES Cyber Systems and not all internal communications within a facility network at a discrete location.

We also suggest that the Project Scope language be modified (bold text) as follows:

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications assets to networks containing low impact BES Cyber Systems from Cyber Assets outside the assets, for those assets with external routable connectivity.

Additionally, we suggest that the third bulleted recommendation contained in the Detailed Description section of the SAR include the following modification (bold text) to address our concern regarding the intended scope.

Requirement(s) for detection of malicious communications to/between sent to or from networks assets containing low impact BES Cyber Systems from Cyber Assets outside the asset, at assets with external routable connectivity.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

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

Likes 0	
Dislikes 0	

Response

Michelle Amarantos - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

AZPS agrees with and the proposed scope, however we believe that the use of the CIP-002 categorization language “asset that contains a low impact BES Cyber Systems” may lead to confusion. Modifications should only address communications to low impact BCS at an asset. An asset may contain networks or communications unrelated to the low impact BCS. These unrelated networks appear to be within scope with the current language.

We suggest the Project Scope language be modified as follows:

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications at assets containing low impact BES Cyber Systems with external routable connectivity. Modifications will only address communications from outside the asset to low impact BES Cyber Systems with external routable connectivity.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Quebec (HQ) - 1 - NPCC

Answer	Yes
Document Name	

Comment

While we agree with the overall proposed scope, we offer the following comments as suggsted improvements:

The proposed scope depends on the definition of “external routable connectivity” which is not a defined term and is not part of this SAR’s scope. Recommend this SAR’s scope expand by including what “low impact BES Cyber Systems at assets containing those systems that have external routable connectivity” means. A NERC-defined term should be capitalized. In this SAR, every instance of “external routable connectivity” is lowercase which suggests the SAR is not using a defined term. The NERC-defined term depends on ESP. Lows do not have ESPs. Lending more credibility to the conclusion this SAR is not using a defined term. This SAR’s source is the Low Impact Criteria Review Team report which includes “Electronic Access Controls” as a risk which includes “require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset.” Most CIP-003 interpretations were for the location, not the asset. Both auditors and implementers need a consistent interpretation. What is the boundary? How does one know internal vs external?

Request one term with a definition instead of “remote” and “external.” We need clarification of remote/external to what?
Consider the impact of “demarcation of” / “asset boundary” in CIP-003
Request clarification of other terms used in CIP-003. Suggest this is an opportunity to consolidate terms and reduce industry confusion
User-initiated interactive access (CIP 3 Reference Model 5, concerning Low Impact)
Inbound and outbound electronic access (CIP 3, Section 3)
Inbound electronic access (CIP 3 Reference Model 5, concerning Low Impact)
Indirect access (CIP 3 Reference Model 6,9)
Vendor electronic remote access (proposed CIP 3)
Lower case “erc” that the SAR proposes
Does this include system-to-system? Does this include Interactive Remote Access?

Likes 0	
Dislikes 0	

Response	
Lori Frisk - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports the comments provided by Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	Yes
Document Name	
Comment	

While we agree with the overall proposed scope, we offer the following comments as suggested improvements.

The proposed scope depends on the definition of “external routable connectivity” which is not a defined term and is not part of this SAR’s scope. Recommend this SAR’s scope expand by including what “low impact BES Cyber Systems at assets containing those systems that have external routable connectivity” means. A NERC-defined term should be capitalized. In this SAR, every instance of “external routable connectivity” is lowercase which suggests the SAR is not using a defined term. The NERC-defined term depends on ESP. Lows do not have ESPs. Lending more credibility to the conclusion this SAR is not using a defined term. This SAR’s source is the Low Impact Criteria Review Team report which includes “Electronic Access Controls” as a risk which includes “require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset.” Most CIP-003 interpretations were for the location, not the asset. Both auditors and implementers need a consistent interpretation. What is the boundary? How does one know internal vs external?

Request one term with a definition instead of “remote” and “external.” We need clarification of remote/external to what?
Consider the impact of “demarcation of” / “asset boundary” in CIP-003
Request clarification of other terms used in CIP-003. Suggest this is an opportunity to consolidate terms and reduce industry confusion
User-initiated interactive access (CIP 3 Reference Model 5, concerning Low Impact)
Inbound and outbound electronic access (CIP 3, Section 3)
Inbound electronic access (CIP 3 Reference Model 5, concerning Low Impact)
Indirect access (CIP 3 Reference Model 6,9)
Vendor electronic remote access (proposed CIP 3)
Lower case “erc” that the SAR proposes
Does this include system-to-system? Does this include Interactive Remote Access?

Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Kuehne - AEP - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

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	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC	
Answer	Yes
Document Name	
Comment	
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	
The proposed scope depends on the definition of “external routable connectivity” which is not a defined term and is not part of this SAR’s scope. Recommend this SAR’s scope expand by including what “low impact BES Cyber Systems at assets containing those systems that have external	

routable connectivity” means. A NERC-defined term should be capitalized. In this SAR, every instance of “external routable connectivity” is lowercase which suggests the SAR is not using a defined term. The NERC-defined term depends on ESP. Lows do not have ESPs. Lending more credibility to the conclusion this SAR is not using a defined term. This SAR’s source is the Low Impact Criteria Review Team report which includes “Electronic Access Controls” as a risk which includes “require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset.” Most CIP-003 interpretations were for the location, not the asset. Both auditors and implementers need a consistent interpretation. What is the boundary? How does one know internal vs external?

Request one term with a definition instead of “remote” and “external.” We need clarification of remote/external to what?

Consider the impact of “demarcation of” / “asset boundary” in CIP-003

Request clarification of other terms used in CIP-003. Suggest this is an opportunity to consolidate terms and reduce industry confusion

User-initiated interactive access (CIP 3 Reference Model 5, concerning Low Impact)

Inbound and outbound electronic access (CIP 3, Section 3)

Inbound electronic access (CIP 3 Reference Model 5, concerning Low Impact)

Indirect access (CIP 3 Reference Model 6,9)

Vendor electronic remote access (proposed CIP 3)

Lower case “erc” that the SAR proposes

Does this include system-to-system? Does this include Interactive Remote Access?

Likes 0	
Dislikes 0	

Response

2. Provide any additional comments for the SAR drafting team to consider, if desired.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC	
Answer	
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
We would like to thank the SDT for allowing us to provide feedback.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
The current scope wording could require implementation of complex, time-consuming solutions that could negatively impact reliability with minimal security benefit. Adding these specific technical requirements to CIP-003-9 may cause confusion with similar requirements currently included in CIP-005-7 and CIP-007-6. Including these detailed, technical requirements in CIP-003-9 instead of with other ESP controls in CIP-005-7 increases the likelihood of non-compliance because CIP-003-9 is intended to define security management controls at the cyber program level rather than at the detailed technical level. In addition, we suggest clarification on the Detailied Description to Modify CIP-003-9 to include:	

Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.

Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

NST suggests the following:

New requirement(s) for "protection of user authentication information in transit" should specify what such protections are meant to accomplish, e.g., "confidentiality protection for user authentication information in transit."

New requirement(s) for "detection of malicious communications to/between assets" containing low impact BES Cyber Systems" should be "to or from assets containing low impact BES Cyber Systems."

The SAR's "Date Submitted" field appears to have a typo.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5

Answer	
Document Name	

Comment

We agree Project 2023-04 (Modifications to CIP-003) impacts 2016-02 (Modifications to CIP Standards) and 2021-03 (CIP-002 Transmission Owner Control Centers). The industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. It appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing Project 2016-02 project and the proposed Project 2021-03 projects, we previously recommended that Project 2016-02 completes before Project 2021-03 project proceeds. We extend this recommendation to Projects 2023-04 and 2023-05 (Internal Network Security Monitoring) because CIP Requirements and definitions are deeply intertwined. Correcting

one issue has caused issues elsewhere. Multiple projects updating the same Requirements and definitions cost the industry money. Entities invest in implementing the new language. Only to see that investment lost a few months later when another project changes that language – see LERC and LEAP.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 5,6	
Answer	
Document Name	
Comment	
Constellation has no additional comments Kimberly Turco on behalf of Constellation Segments 5 and 6	
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 Project 2023-04 (Modifications to CIP-003) impacts 2016-02 (Modifications to CIP Standards) and 2021-03 (CIP-002 Transmission Owner Control Centers). The industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. It appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing Project 2016-02 project and the proposed Project 2021-03 projects, we previously recommended that Project 2016-02 completes before Project 2021-03 project proceeds. We extend this recommendation to Projects 2023-04 and 2023-05 (Internal Network Security Monitoring) because CIP Requirements and definitions are deeply intertwined. Correcting one issue has caused issues elsewhere. Multiple projects updating the same Requirements and definitions cost the industry money. Entities invest in implementing the new language. Only to see that investment lost a few months later when another project changes that language – see LERC and LEAP.	
Likes 0	

Dislikes 0	
Response	
Chantal Mazza - Hydro-Quebec (HQ) - 1 - NPCC	
Answer	
Document Name	
Comment	
We agree Project 2023-04 (Modifications to CIP-003) impacts 2016-02 (Modifications to CIP Standards) and 2021-03 (CIP-002 Transmission Owner Control Centers). The industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. It appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing Project 2016-02 project and the proposed Project 2021-03 projects, we previously recommended that Project 2016-02 completes before Project 2021-03 project proceeds. We extend this recommendation to Projects 2023-04 and 2023-05 (Internal Network Security Monitoring) because CIP Requirements and definitions are deeply intertwined. Correcting one issue has caused issues elsewhere. Multiple projects updating the same Requirements and definitions cost the industry money. Entities invest in implementing the new language. Only to see that investment lost a few months later when another project changes that language – see LERC and LEAP.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy seeks the SAR’s direction to cross check all existing projects for potential encompassing of standards that may be affected.	
Likes 0	
Dislikes 0	
Response	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	

Xcel Energy supports the comments of EEI and MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	
Document Name	
Comment	
N/A Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA suggests adding “Where capable” or “Where technically feasible” to these requirements. Low sites often have the most outdated technology and some of the controls recommended may not be doable at the sites.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group	
Answer	
Document Name	
Comment	

WEC Energy Group supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	

Comment

The NAGF does not have any additional comments.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power

Answer	
Document Name	

Comment

Tacoma Power recommends that when developing the CIP-003-X redlines, the SDT should provide additional clarification as to how these changes are different than the work being performed in response to the FERC Order on internal network security monitoring. As currently written in the SAR, it's not clear whether Project 2023-04 will address internal (east-west) or external (north-south) network monitoring.

Additionally, the SDT should consider if there's a security benefit to monitoring encrypted communications and if there are benefits, how entities will monitor these encrypted communications.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
ATC requests NERC consider the timing of this SAR alongside the emerging study to evaluate Internal Network Security Monitoring (INSM) for low impact, as well as the inflight effort for 2016-02 to enable for virtualization. Having multiple drafting teams focused on modifications to the same CIP Standard creates potential for confusion and reduces the ability to attain steady state for these regulations. ATC also supports EEI and NSRF comments.	
Likes 1	Tacoma Public Utilities (Tacoma, WA), 1,3,4,5,6, Wike Jennie
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	

Comment
The MRO NSRF has concerns with the use term “external routable connectivity” There is already a defined term External Routable Connectivity that applies to high and medium-impact BES Cyber Systems and not to low impact. The term used on this SAR has a different meaning or is applied in a different way than for the defined term. For this reason, the MRO NSRF requests that the drafting team either uses a different term or defines low impact External Routable Connectivity.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	

Comment
MISO supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	

Comment
None

Likes 0	
Dislikes 0	

Response