Comment Report

Project Name:	2020-03 Supply Chain Low Impact Revisions | Standard Authorization Request
Comment Period Start Date:	4/3/2020
Comment Period End Date:	6/3/2020
Associated Ballots:	

There were 49 sets of responses, including comments from approximately 106 different people from approximately 84 companies representing 8 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
Santee Cooper	Chris Wagner	1,3,5,6		Santee Cooper	Robert Rhett	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Andy Crooks	SaskPower Corporation	1	MRO
					Bryan Sherrow	Kansas City Board of Public Utilities	1	MRO
					Bobbi Welch	Omaha Public Power District	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Bobbi Welch	Midcontinent ISO	2	MRO
					Douglas Webb	Kansas City Power & Light	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO
					James Williams	Southwest Power Pool, Inc.	2	MRO
					Jamie Monette	Minnesota Power / ALLETE	1	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Sing Tay	Oklahoma Gas & Electric	1,3,5,6	MRO

					Terry Harbour	MidAmerican Energy	1,3	MRO
					Troy Brumfield	American Transmission Company	1	MRO
Westar Energy	Douglas Webb	1,3,5,6	MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jim Davis	East Kentucky Power Cooperative	1,3	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Scott Brame	North Carolina EMC	3,4,5	SERC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
					Carl Behnke	Southern Maryland Electric Cooperative	3	RF
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
FirstEnergy - FirstEnergy Corporation	Mark Garza	1,3,4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF

					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Northern California Power Agency	Marty Hostler	3,4,5,6		NCPA	Michael Whitney	Northern California Power Agency	3	WECC
					Scott Tomashefsky	Northern California Power Agency	4	WECC
					Dennis Sismaet	Northern California Power Agency	6	WECC
					Marty	Northern California Power Agen	5	WECC
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
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
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC

Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Lower Colorado River Authority	Teresa Cantwell	1,5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

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.

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6

Answer	No
Document Name	

Comment

Some smaller agencies rely soely on thrid parties to proved all of the cyber services because they do not have a Information Technology department or staff. Extending the proposed requirments down to smaller utilities, such as monitoring remote access, will have a significant burden on these utilities. They will not have the resources to manage a standard like this.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Detection of "known or suspicious malicious communications" should only apply to "active vendor remote access sessions." That is, normal data communications between BES Cyber Systems inside the asset and cyber systems outside should not be part of the scope of this proposal as they have nothing to do with the supply chain. This may be what is intended in this proposal but it is not clearly stated.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

Extending the proposed requirements to low impact facilities will have a significant financial and resource management burden on utilities.

Likes 0	

Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

- These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments".

The NSRF agrees this SAR is for policy inputs for low impact BES Cyber Systems that allow 3rd party vendor remote access. The first point to be contained in a policy is unclear.

"(1) detect known or suspected malicious communications for both inbound and outbound communications". We don't know what "malicious communication" is meaning within this first attribute? The Supply Chain Risk Assessment Report (linked within the SAR) only uses "malicious", twice. Once in the Background section and once in foot note 15. Both instances do not describe what "malicious communication" is or how it could be applied. Without a clear understanding of what the intent of "malicious communications" is, the Standard Drafting Team may not satisfy the intent of the NERC BOT and the Supply Chain Risk Assessment Report. Does "malicious" cover every type of act that could do harm? From physical to cyber (DOS, Phishing, malware, social engineering, cutting communication cables, etc.)?

We also question why the first attribute wants the detection of "known and suspected" since both are considered malicious. Recommend that "known and suspected" be deleted and it will now read "(1) detect malicious …".

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

N&ST recommends against the proposed modification of CIP-003-8 to include policies for low impact BES Cyber Systems to detect known or suspected malicious communications for both inbound and outbound communications (Item 1, above), for the following reasons:

- At the present time this requirement, as established by CIP-005-6 R1 Part 1.5, applies only to High and Medium impact BES Cyber Systems at Control Centers. Adding a similar requirement to CIP-003-8 would result in some assets with Low Impact BES Cyber Systems being subject to more stringent communication security requirements than apply to Medium Impact BES Cyber Systems with External Routable Connectivity at BES assets other than Control Centers.

- There is no explicit statement of concern about "known or suspected malicious communications" in the NERC Supply Chain Risk Assessment final report.

- As written, the SAR could lead to a “malicious communication detection” requirement for Low Impact assets with BES Cyber Systems REGARDLESS of whether or not they allow “vendor remote access.”

N&ST also recommends modifying the SAR to address the following concerns:

- It should be clear that new requirements for “vendor remote access” will apply only to those BES assets that (1) contain Low Impact BES Cyber Systems and (2) are subject to the existing electronic access control requirements in CIP-003-8 Attachment 1, Section 3.

- Any and all supply chain - related terms introduced in a revised version of CIP-003 should be consistent with terms already used in CIP-005-6. N&ST noted the SAR refers to both “vendor remote access,” which appears in CIP-005-6, and “3rd party remote access,” which does not appear in CIP-005-6. N&ST strongly believes the latter phrase should not be used, as it would likely sow confusion about requirement applicability.

- Regarding the draft SAR’s statement about potential costs, “Cost impact is unknown at this time,” N&ST believes that new requirements to detect and manage “vendor remote access” may, for some entities, require a complete overhaul of their existing Low Impact electronic access control implementations, significant investments in new networking equipment, or both.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

RF is in agreement with the three items in the proposed scope for this SAR, but we think the scope should include mitigation for supply chain cyber security risk for low impact. This could include in current Supply Chain Cyber Security Risk Management plan for high and medium impact BES Cyber Systems or something just for low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

In the Industry Need, request replace “third party” with “vendor” for consistency with the rest of this SAR.

In the Goals section, we disagree with the inclusion of Goal #1 in the SAR, to “detect known or suspected malicious communications for both inbound and outbound communications” for the following reasons:

1) This provision is not included as a recommendation in the “NERC Supply Chain Risk Assessment Report (December 2019).”

2) The CIP-005, requirement that aligns with this goal is for Control Centers only.

3) The current wording of this goal would apply to all communications and not just those paths used for vendor remote access or even just those that use ERC.

Applying Goal 1 to low impact facilities is inconsistent with the stated purpose of the SAR and overly burdensome on low impact Facilities.

CIP-005 allows for TFEs for the medium and high impact requirements that align with Goals #2 and #3. Consideration should be given to the handling of TFEs at low impact Facilities. With the number of low impact Facilities that are going to apply these requirements, using the TFE process would be overly burdensome and not provide a significant benefit to reliability.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not agree with the proposed scope as described in the SAR. Duke Energy supports the overall intent to modify CIP-003-8 to include policies for mitigating risks posed by third party electronic access to low impact BES Cyber Systems or Assets containing those systems.

Duke Energy recommends clarification of the project scope and purpose to move forward with an approach that characterizes the risks to the BES, as a whole, posed by 3rd party access to low impact BES Cyber Systems or Assets containing those systems. Duke Energy recommends such a risk characterization be employed to provide an appropriate risk informed mitigation. The detailed description as written implies a solution that may impose significant burden on owners with existing system architectures which may not support the required modifications, or be may not be commensurate with the actual risk.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC believes the scope as written is too broad and ccould be written to better align with the intent of the SAR.

Potential suggestions would be:

(2) implement methods to monitor for and detect known or suspected vendor-initiated malicious communications for both inbound and outbound communications;

(1) implement methods to determine when active vendor remote access sessions are initiated; and

(3) disable active vendor remote access when necessary.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

Although the CAISO acknowledges that low impact BES Cyber Systems with remote electronic access connectivity are important to protect in line with the FERC Order, we recommend to wait on extending the program to them until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years to allow for the processes and controls to mature and to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors. At that time, the CAISO also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

The proposed SAR for CIP-003 changes are specific to electronic access controls for vendor remote access, but the SAR does not address introduced and increased risk of supply chain procurements of low impact BES Cyber Systems. Vendors remotely accessing sites/assets and the associated low impact BES Cyber Systems present a substantial risk, but the proposed new requirements do not address vulnerabilities vendors may introduce to low impact BCS, ranging from potential compromised access, revocation of vendor access, no awareness of vendor incidents, no disclosure of known vulnerabilities related to products used with low impact BCS, etc. For example, entities without awareness of a vendor's vulnerabilities or coordination of responses to incidents could impact countless low impact BCS across several registered entities throughout Interconnections.

NERC's December 2019 report affirms a coordinated attack across low impact BES Cyber Systems could introduce significant adverse impact on reliability. Simply defining access controls for vendors does not mitigate other notable risks introduced with the supply chain of products and services supporting low impact BCS. For low impact sites/assets, several vendors are used for maintenance and operation functions and responsibilities. The absence of a proper risk assessment of vendor services and/or products for low impact BES Cyber Systems could potentially have an adverse impact to the BES. The SAR should be revised to ensure inclusion of low impact BCS with supply chain risk management.

Further, with the recent publication of the Executive Order Number 13920, the SAR should be expanded to include supply chain risk management with low impact BES Cyber Systems. It is a growing risk and initiating forward momentum in Project 2020 03 could assure alignment of the ERO with all impacted bulk power industries, not just those affiliated with NERC.

Likes 0	
Dislikes 0	
Response	

Douglas Webb - Westar Energy - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	

Evergy (Westar Energy and Kansas City Power & Light), incorporate by reference and support the Edison Electric Institute (EEI) response to Question 1.

Likes 0	
Dislikes 0	
Response	

Tony Skourtas - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	No
Document Name	
Comment	

The policy to detect malicious communications will be a significant increase in user action for the low-impact category and is in contrast to the nominal NERC CIP approach, which uses an asset-centric, risk-based method. As the NERC Report indicated, the risk based scores from the survey data are low.

This Standard revision is occurring as part of the supply chain risk management efforts, but it seems like the scope exceeds vendor remote access to low-impact BES assets. Further clarification on applicability is needed.

Likes 0	
Dislikes 0	
Response	

Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	

AEP does not agree with the scope of the proposed SAR as written, as it currently appears to use the terms “vendor” and “3rd party” interchangeably. Indeed, the Supply Chain Risk Assessment also appears to use these terms as one in the same, which likely resulted in the “Goal and Purpose” of the SAR referring to **vendor** access, while the “Detailed Description” refers to locations with **3rd party** remote access.

As such, the proposed SAR is unclear in it stated purpose. AEP believes that should this project move forward, that the terms “vendor” and “3rd party” would need to be formally defined, and that work should take place either prior to, or in conjunction with, this project. This will provide the industry the clarity needed to fully understand and implement any requirement(s) developed in the revised Standard.

As reference, a “vendor” is typically an independent entity that provides a service or product, and may or may not be vetted for their security posture. While a “3rd party” can be a person or entity that is a contractor for a registered entity that performs certain duties, and has been vetted with the same scrutiny as employees, or even a neighboring utility employee that has the need to access information from a common facility.

It also worth noting that FERC Order 829, which directed NERC to develop the Supply Chain Standards, refers to mitigating vendor risk, specifically it states:

“[FERC directs] “*NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, discussed in detail [in the Order]: (1) software integrity and authenticity; (2)* ***vendor*** *remote access; (3) information system planning; and (4)* ***vendor*** *risk management and procurement controls.”*

Likes 0	

Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The Project 2020-03 on Supply Chain Low Impact Revisions will continue to distort the primary goal of the NERC CIP-003 Standard, which is Security Management Controls. Most of the requirements in this standard are about “Management”. By continuing to address Low Impact BES Cyber Systems (L-BCS) within the CIP-003, we distort the standard.

Requirements 1, 3 and 4 of CIP-003 are about real management concerns: what is subject to CIP Senior Manager’s approval, the identification of a CIP Senior Manager and its authority delegation. R2 of CIP-003 is about L-BCS and don’t have its place into CIP-003.

As we are going to address L-BCS almost like M-BCS or H-BCS, we should address L-BCS like High and Medium BCS. We should status if a given requirement is applicable to Low (L-BCS). If yes, add it in the “Applicable Systems” column of the given requirement. I don’t understand why we have to make an exception of L-BCS.

The new requirement “(1) detect known or suspected malicious communications for both inbound and outbound communications” for Electronic Access Points (EAP) for L-BCS already exists as R1.5 in CIP-005 standard for EAP of M-BCS at control centers and EAP of H-BCS. Doing this is a non-sense if we apply the requirement to all EAP for L-BCS without applying that requirement to all EAP for M-BCS.

The new requirement “(2) determine when active vendor remote access sessions are initiated” is almost similar to R1.3 (and R1.4 maybe) in CIP-005 standard on EAP for M-BCS and H-BCS.

The new requirement “(3) disable active vendor remote access when necessary” is similar to a part of R1.3 in CIP-005 standard on EAP for M-BCS and H-BCS: “… deny all other access by default”. At least, it could be a new requirement of CIP-005 standard, dedicated to EAP for L-BCS.

With the Transient Cyber Asset (TCA) used on L-BCS: because CIP-010 is covering TCA used on M-BCS, why didn’t we group together TCA used on L-BCS? WE should keep the concerns of the same nature all together. Many times, TCA used on M-BCS will be used or could be also used on some L-BCS. Using CIP-003 to cover TCA used on L-BCS and CIP-010 to cover TCA used on M-BCS is a non-sense.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - NAGF - 6 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

NAGF Comments:

We agree with need to address the risk to the grid from low-impact remote access and therefore with the intent of the SAR. However, the requirements that could come out of the SAR, the way that it is currently written could result in low-impact generation entities facing stricter requirements than medium-impact generation entities. In addition, the requirements that could result from the SAR, as it is currently written, could be a significant cost to organizations requiring retrofit of existing systems and could require contract negotiations with vendors. To address these, and other concerns, we would like to see the following considered in a revised SAR and/or in the draft standard itself:

1. **SAR Scope & Detailed Description**:

The "Project Scope" section of the SAR does not set a clear enough scope for the project. This section should be modified to direct the creation of a standard or revision of a standard to address the security objective of mitigating the risk posed by vendor/3rd party remote access to assets containing low impact BES Cyber Systems while still allowing the entity flexibility in how to meet these objectives.

Consistent with the wording used in the CIP-002 (and CIP-003) standards the "**Detailed Description**" section be modified from "low impact BES Cyber Systems at locations" to "assets containing low impact BES Cyber Systems". Concerns with the specific security requirements (1-3) included in the Detailed Description section have been outlined below. It is also noted that this section switches terms from "vendor" to "3rd party", this should be corrected to be consistent and defined.

2. Diversity of Bulk Electric System low impact entities:

The SAR should be written in a manner that will result in a standard that does not impose ''one-size fits all'' language. Within the low-impact category there are significant differences that exist among entities and this standard must be flexible enough to account for the differences in the needs and characteristics of responsible entities, the diversity of the Bulk Electric System environments, technologies, risks and issues related to the limited applicability of mandatory NERC reliability standards. In keeping with FERC Order No. 829, the SAR should accommodate different controls based on the criticality of different assets. This flexibility in the 2016-03 SAR allowed the SDT to apply the requirement for medium and high impact entities to detect malicious communication both inbound and outbound (CIP-005-5 R1.5) at varying degrees depending on risk to the grid.

- **Security Requirement 1: Detect known or suspected malicious communications for both inbound and outbound communications**

A similar requirement exists under CIP-005-5 R1.5 for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers. Imposing this regulation on low impact BES Cyber Systems before it is imposed on the entirety of medium impact cyber systems does not correlate with NERC's risk-based approach to compliance. This issue could be rectified if the SAR was amended to include more security objective language vs. specific security requirements as it does currently. As this security requirement is currently written it will require significant resources, rework / replacement of infrastructure recently installed and installation of new systems that are not required for higher risk medium impact generation registrations.

- **Security Requirement 2: Determine when active vendor remote access sessions are initiated**

For renewable sites that rely on OEM providers for ongoing maintenance and operational support, vendor remote access is required frequently. In some situations, especially where operational personnel are not on site 24/7 this vendor remote access is vital to ensuring that these largely dispersed, and often unmanned sites can actively support the reliability of the grid. We encourage the Standard Drafting Team to consider these situations and ensure the standard allows enough flexibility to accommodate.

We recommend that the SAR be revised to address the type of remote access that would be applicable to this requirement and expressly indicate if it is all remote access or is focused solely on Interactive Remote Access.

- **Security Requirement 3: Disable active vendor remote access when necessary**

We recommend that the Standard Drafting Team consider the physically remote locations of many low impact assets and the potential challenges applying this security requirement.

Likes 0	

Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	

Comment
San Miguel Electric Cooperative agrees with the comments submitted by Barry Lawson of NRECA. We agree with the intent to protect the Low - BCS from supply chain risks, but the SAR is written with detailed requirements that are not one-size fits all nor risk-based. Entities should evaluate the vulnerabilities/risks, and have flexibility on how to address them. The detailed requirements as written could result in Low-BCS requirements being more stringent than those for Medium-BCS. Entities should be required to evaluate risks and define needed controls. Any specific requirements should only apply to active vendor remote access that is not part of a normal or constant communication or monitoring service.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	

Comment
The language for (2) and (3) needs to match what was defined for CIP005-6 R2 Part 2.4 and Part 2.5. This ensures that the standards are consistent for High, Medium, and Low impact BCS that all External Routable Connectivity. Otherwise the language is vague and will lead to ineffective standards.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	

Comment

The proposed revisions bullet (1) “detect known or suspected malicious communications for both inbound and outbound communications” is directly borrowed from CIP-005-5 R1.5 for high and medium impact BCS, which has no direct linkage with bullet (2) & (3). If you want to link bullet (1), (2) and (3) together, we suggest changing the bullet (3) as follows:

“(3) disable active vendor remote access when the malicious communications are detected.”

The bullet (1) will bring a significant cost to industry for deploying IDS/IPS at low impact BCS sites with external routable connectivity. If this requirement is only based on a perception of an “aggregate misuse of numerous low impact BCS.”, we suggest developing a criterion to identify the aggregate points of low impact sites rather than applying this requirement to all low impact sites.

Likes 0	
Dislikes 0	

Response

Shannon Ferdinand - Capital Power Corporation (MRRE 80) - NA - Not Applicable - MRO,WECC,Texas RE,NPCC,SERC

Answer	No
Document Name	

Comment

We agree with need to address the risk to the grid from low-impact remote access and therefore with the intent of the SAR. However, the requirements that could come out of the SAR, the way that it is currently written could result in low-impact generation entities facing stricter requirements than medium-impact generation entities. In addition, the requirements that could result from the SAR, as it is currently written, could be a significant cost to organizations requiring retrofit of existing systems and could require contract negotiations with vendors. To address these, and other concerns, we would like to see the following considered in a revised SAR and/or in the draft standard itself

1. **SAR Scope & Detailed Description**:

The “Project Scope” section of the SAR does not set a clear enough scope for the project. This section should be modified to direct the creation of a standard or revision of a standard to address the security objective of mitigating the risk posed by vendor/3rd party remote access to low impact BES Cyber Systems while still allowing the entity flexibility in how to meet these objectives.

Consistent with the wording used in the CIP-002 (and CIP-003) standards the “**Detailed Description**” section be modified from “low impact BES Cyber Systems at locations” to “assets containing low impact BES Cyber Systems”. Concerns with the specific security requirements (1-3) included in the Detailed Description section have been outlined below. It is also noted that this section switches terms from “vendor” to “3rd party”, this should be corrected to be consistent and defined.

2. Diversity of Bulk Electric System low impact entities:

The SAR should be written in a manner that will result in a standard that does not impose ‘‘one-size fits all’’ language. Within the low-impact category there are significant differences that exist among entities and this standard must be flexible enough to account for the differences in the needs and characteristics of responsible entities, the diversity of the Bulk Electric System environments, technologies, risks and issues related to the limited applicability of mandatory NERC reliability standards. In keeping with FERC Order No. 829, the SAR should accommodate different controls based on the criticality of different assets. This flexibility in the 2016-03 SAR allowed the SDT to apply the requirement for medium and high impact entities to detect malicious communication both inbound and outbound (CIP-005-5 R1.5) at varying degrees depending on risk to the grid.

Security Requirement 1: Detect known or suspected malicious communications for both inbound and outbound communications

A similar requirement exists under CIP-005-5 R1.5 for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers. Imposing this regulation on low impact BES Cyber Systems before it is imposed on the entirety of medium impact cyber systems does not correlate with NERC's risk-based approach to compliance. This issue could be rectified if the SAR was amended to include more security objective language vs. specific security requirements as it does currently.

As this security requirement is currently written it will require significant resources, rework / replacement of infrastructure recently installed and installation of new systems that are not required for higher risk medium impact generation registrations.

Security Requirement 2: Determine when active vendor remote access sessions are initiated

For renewable sites that rely on OEM providers for ongoing maintenance and operational support, vendor remote access is required frequently. In some situations, especially where operational personnel are not on site 24/7 this vendor remote access is vital to ensuring that these largely dispersed, and often unmanned sites can actively support the reliability of the grid. We encourage the Standard Drafting Team to consider these situations and ensure the standard allows enough flexibility to accommodate.

We recommend that the SAR be revised to address the type of remote access that would be applicable to this requirement and expressly indicate if it is all remote access or is focused solely on Interactive Remote Access.

We recommend that if discrete security requirements such as this are incorporated into the standard, that the SDT try to ensure consistency in language, were possible, with other similar requirements (i.e. CIP-005-7 proposed language for R3 3.1: Have one or more methods for detecting vendor-initiated remote access sessions).

Security Requirement 3: Disable active vendor remote access when necessary

We recommend that the Standard Drafting Team consider the physically remote locations of many low impact assets related to any timeframe requirements associated with this requirement and the speed at which an entity may be able to disable vendor remote access.

We recommend that the standard add clarity regarding thresholds for determining the necessity of termination.

We recommend that if discrete security requirements such as this are incorporated into the standard, that the SDT try to ensure consistency in language, were possible, with other similar requirements (i.e. CIP-005-7 proposed language for R2 2.5 Have one or more method(s) to terminate established vendor-initiated remote access sessions).

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

Frist, Oncor suggests using "assets containing low impact BES Cyber System" rather than "low impact BES Cyber Systems at locations" in consistent with the current CIP-002 language.

Second, current requirement doesn't require to produce a list of low impact BES Cyber System. However, in order to fulfill the goals listed in the SAR, responsibility entity may have to create an inventory of low impact BES Cyber System and its associated software, hardware which would be difficult and over burden due to the high number of low impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the comments made by EEI.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
If these changes were accepted, this requirement would be more stringent than what is currently required for Medium Impact BCS and on par with the requirements for EAPs for Medium Impact Control Centers and High Impact BCS. We would not be in favor of elevating requirements for Medium Impact BCS in the future and are not in favor of this change for Low Impact BCS. Registered Entities (REs) recently completed their implementation of CIP-003-7 for Low Impact BCS. While the requirements in CIP-005 are best Cyber Security practices for Low Impact BCS, REs with only Low Impact BCS do not fall under CIP-005 compliance and do not always have systems, which would allow them to determine when active vendor remote access sessions are initiated (item #2) and disable active vendor remote access when necessary (item #3). This would require significant investment and management of remote access (if allowed by the RE), especially for small entities who are already resource-constrained. Further, Item #2 and Item #3 do not align with the Supply Chain Cyber Security risk management, but fall into the Electronic Access Controls area. These suggested changes do not enhance Supply Chain Cyber Security risk management for Low Impact BCS. Therefore, we do not see how these changes align with the scope of the background information provided for the scope of the SAR. The suggested requirements are purely Cyber Security related and do not pertain to Supply Chain Cyber Security risk management, nor the scope of the 1600 Data Request, and should be limited to the scope of FERC Order No. 829.	
Likes 0	

Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 3,4,5,6, Group Name NCPA

Answer	No
Document Name	

Comment

The following are technical reasons why NCPA does not support the subject SAR in its current form:

1. NERC's response to Market Principle 1 on SAR page 3 is inaccurate. CIP-003-8 will result in an unfair competitive advantage for non-GOPs in Regions that have BA/ISOs that don't allow GOPs to recover unfunded FERC mandated NERC compliance program fixed costs.

- California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs.
- If this SAR is to move forward FERC needs to level the playing field and first order BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs.
- Otherwise, at a minimum, this proposed Standard, among others, results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs.
- This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs.

2. NERC has not provided a cost estimate for this proposal. Future SARs should not be allowed though the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting.

3. The President recently signed an Executive Order. The DOE is responsible for BES Supply Chain issues not FERC/NERC. Regardless, FERC, NERC, and Regional Entities still have not agreed how to enforce existing CIP-13 Standards that were to be effective July 1, 2020. In fact, they have ordered changes to CIP-005, 10, and 13, that no one can agree on either. Now they propose even more Supply Chain Standards.

If this SAR does move forward it should require the future CIP STD to not only develop standards, but develop guidance and audit approach measures, that Auditors shall be required to follow. And all of these need to be approved at the same time. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

4. We AGREE with Utility Services (Brian Evan Mongeon's) comments related to this SAR being inconsistent with prior stated goals, among other issues, which we will leave for others to discuss.

Likes 0	
Dislikes 0	

Response

Barry Jones - Western Area Power Administration - 9 - MRO,WECC

Answer	No

Document Name	

Comment

"(1) detect known or suspected malicious communications for both inbound and outbound communications". We don't know what "malicious communication" is meaning within this first attribute? The Supply Chain Risk Assessment Report (linked within the SAR) only uses "malicious", twice. Once in the Background section and once in foot note 15. Both instances do not describe what "malicious communication" is or how it could be applied. Without a clear understanding of what the intent of "malicious communications" is, the Standard Drafting Team may not satisfy the intent of the NERC BOT and the Supply Chain Risk Assessment Report. Does "malicious" cover every type of act that could do harm? From physical to cyber (DOS, Phishing, malware, social engineering, cutting communication cables, etc.)?

We also question why the first attribute wants the detection of "known and suspected" since both are considered malicious. Recommend that "known and suspected" be deleted and it will now read "(1) detect malicious …".

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3,4,5,6

Answer	No
Document Name	

Comment

WEC Energy Group concurs with and supports the EEI comments.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

This requirement could be addressed under the current CIP-003-8 Policy R1.2.3 Electronic access controls. The requirement should be specified under Attachment 1 Section 3, proposed here as a new part within Section 3 referencing malicious communications detection - "at locations that allow 3rd party remote access, have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications to low impact BES Cyber Systems where Cyber Asset(s), as specified by the Responsible Entity, provide electronic access control(s) implemented for Section 3.1."

(2) determine when active vendor remote access sessions are initiated;

This requirement could be addressed under the current CIP-003-8 Policy R1.2.3 Electronic access controls. The requirement could be specified under Attachment 1 Section 3, proposed here as a new part within Section 3 referencing vendor remote access – “at locations that allow 3rd party remote access, have one or more methods for determining active vendor remote access sessions” Purposefully leaving out the CIP-005-6 inclusion to keep things more generic.

From CIP-005-6 R2.4: *Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).*

(3) disable active vendor remote access when necessary.

This requirement could be addressed under the current CIP-003-8 Policy R1.2.3 Electronic access controls. The requirement could be specified under Attachment 1 Section 3, proposed here as a new part within Section 3 referencing vendor remote access – “at locations that allow 3rd party remote access, have one or more method(s) to disable active vendor remote access sessions” Purposefully leaving out the CIP-005-6 inclusion to keep things more generic.

From CIP-005-6 R2.5: *Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).*

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1 - MRO

Answer	No
Document Name	

Comment

MPC does not support the scope of the current project for the following reasons:

· The scope should be adjusted to include a definition for “vendor remote access”. Currently, this undefined term is open for interpretation. In some cases, the term’s interpretation brings web conferences into scope, even when a vendor does not have interactive access. Additionally, the term excludes other types of third parties that may provide remote support, such as a consultant. Also, if a vendor or other third party is onsite, is access via a jump host considered “vendor remote access”? The term “vendor remote access” should either be defined or replaced with a new, defined term, such as “third-party remote access” or “non-employee remote access”.

· MPC supports comments provided by Brian Evans-Mongeon, On Behalf of: Utility Services, Inc. · MPC supports comments provided by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI supports the proposed NERC Board of Trust (BOT) resolution that directs NERC to initiate a project to modify Reliability Standard CIP-003-8 to include specifically identified policies for low impact BES Cyber System, however, the following items need to be addressed in this SAR before we can support its approval: 1. EEI recommends that the SAR Scope be edited to align with the NERC BOT resolution which focuses on CIP-003-8. 2. EEI recommends that the text in the “Purpose or Goal” section be moved to the “Project Scope” section of the SAR. 3. The “Detailed Description” section appears to propose changes to the standard that would require an entity to create an inventory of low impact BES Cyber Systems and associated software to address the SAR. The existing standard has no obligation to create or produce such an inventory, and there does not appear to be a practicable way to implement the proposed supply chain processes without an inventory and associated inventory monitoring and update processes. Creating such an inventory of low impact BES Cyber Systems, which would be required to demonstrate compliance to the proposed standard, is overly burdensome and would not materially enhance reliability. EEI suggests that this section be revised so that it uses the currently approved wording in CIP-002 (and CIP-003) of “assets containing low impact BES Cyber Systems” rather than “low impact BES Cyber Systems at locations.” This keeps the SAR consistent with CIP-002 R1.3 which requires entities to “[i]dentify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).” EEI suggests changing this section to: Revise CIP-003-8 such that assets containing low impact BES Cyber Systems where the asset allows vendor remote access to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.	
Likes 1	PNM Resources - Public Service Company of New Mexico, 3, Tidwell Trevor
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No

Document Name	

Comment

IESO supports the comments submitted by NPCC

In the Industry Need, request replace “third party” with “vendor” for consistency with CIP-013.

In the Purpose / Goal, #1 is similar to CIP-005 Part 1.5 which is applicable to High / Medium Control Centers. Implementing Goal #1 would result in this requirement not applying to other Medium Impact assets while applying to High and Low. Next, we cannot find this concern as a recommendation in the study. So, we recommend removing Goal #1.

Goal #2 is similar to CIP-005 Part 2.4. Goal #3 is similar to CIP-005 Part 2.5. The corresponding Requirement 2 includes Technically Feasible Exception (TFE) language. If Goals #2 and #3 include TFE language, we do not believe the industry will achieve a desirable result. We recommend including a process for excluding communications based on capabilities without requiring a TFE.

CIP-005 Part 2.4 does not have the language “when initiated.” Recommend consistency with Part 2.4.

Project Scope says there are “recommendations” in the NERC Supply Chain Risk Assessment Report. That report makes only one recommendation. We request that the single recommendation be explicitly included in this Project Scope.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1,3,5 - NPCC

Answer	No
Document Name	

Comment

The Taunton Municipal Lighting Plant supports the comments submitted by Brian Evans-Mongeon of Utility Services, Inc., specifically the following:

In the Goals section, we disagree with the inclusion of Goal #1 in the SAR, to “detect known or suspected malicious communications for both inbound and outbound communications” for the following reasons:

1. This provision is not included as a recommendation in the “NERC Supply Chain Risk Assessment Report (December 2019).”
2. The CIP-005, requirement that aligns with this goal is for Control Centers only.
3. The current wording of this goal would apply to all communications and not just those paths used for vendor remote access or even just those that use ERC.

Applying Goal 1 to low impact facilities is inconsistent with the stated purpose of the SAR and overly burdensome on low impact Facilities.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	No
Document Name	
Comment	

NRECA has several significant and foundational concerns with the SAR and its scope as follows:

1. The proposed modifications are not technically justified or supported. The "NERC Supply Chain Risk Assessment Report (December 2019)" does not provide the necessary technical justification for the proposed scope of the SAR. The Cooperative Sector and NRECA provided detailed policy input to the NERC BOT for the February 2020 BOT meeting detailing our issues with the report's recommendation. This SAR appears to rely on that report for its technical justification and support, and, for that reason, NRECA respectfully re-asserts the following regarding its concerns about the justification for the proposed SAR:

a. The supply chain data request asked entities how their CIP-013-1, requirement R1 plan will affect low impact BES Cyber Systems and to describe the methods they intended to use to apply such plan to low impact BES Cyber Systems. This extremely narrowly-focused question did not allow for entities to provide any insight or guidance into other security-related procurement strategies that they may be employing during the procurement of low impact BES Cyber Systems, e.g., security-related contract provisions, third party risk reviews, chain of custody processes, etc. For those entities that have existing security-related procurement strategies that are NOT the result of or directly derived from the entity's specific CIP-013-1, requirement R1 plan, the response to this question would have been negative. However, such response also would not necessarily have been representative of an entity's security risk mitigation strategies for low impact BES Cyber System procurement. Accordingly, the responses gathered, and assumptions made regarding such responses are insufficient to support a determination that low impact BES Cyber Systems are not subject to security risk mitigation strategies during their procurement.

b. Using only the number of asset locations, NERC determined that a coordinated cyber-attack with control of multiple low impact locations could result in an event that has an interconnection-wide BES reliability impact. However, the actual potential for such an impact is closely correlated with the geographic and electrical location of assets within an interconnection, their individualized, aggregate ability for impact within and beyond their local area, the overall electrical configuration within which such issue would arise, and other essential factors and characteristics. Neither number nor any of these additional factors alone are determinative of the likelihood or risk of an aggregate, interconnection-wide reliability impact. Hence, without additional context and evaluation of the low impact assets and their associated low impact BES Cyber Systems, the determination that sheer numbers of locations (regardless of location, size, electrical impact, etc.) would aggregate into an interconnection-wide impact cannot be supported and should not form the basis for the modification of the scope or applicability of a reliability standard.

c. The generalized nature of the third-party access question also does not provide enough information and context for the true risk and potential for impact to be discerned. The risk of third-party access cannot be evaluated in isolation - without an understanding of any processes, controls, or risk mitigation strategies being employed when such access is granted. Given the right processes, controls, and risk mitigation strategies, granting a third-party access may not present any additional risk to the BES. For example, third party entities with access may be other registered electric industry entities with awareness of, and independent responsibility for, cyber security and reliability compliance. Additionally, an entity allowing third party access may have substantial and robust controls, such as background check requirements, continuous escorting, monitoring, or other protective measures. Further, while entities may allow third party access, criteria may be stringent; such access may be rare; and such access may have the effect of reducing risk and enhancing overall reliability. Without more information, there is not a true idea of actual risk to be addressed and mitigated.

d. Further, the current reliability standards for low impact BES Cyber Systems require that specific security controls be implemented to mitigate cyber security risk for these assets. It is unclear from the analysis provided whether NERC evaluated the effect of these required cyber security controls to determine their contribution to the mitigation of cyber security risk and the overall security of the BES.

For these reasons, NERC's finding of increased risk in its December 2019 report is premature and should not be relied upon as a basis for the modification of the scope or applicability of the reliability standards.

2. NRECA views the SAR as overly prescriptive by proposing specific technical requirements for inclusion in CIP-003-8. CIP-003-8 already prescribes a number of security controls be implemented for low impact assets. How or whether these current security controls contribute to or support the intent of these new specifications as well as how these new specifications get incorporated into reliability standards are typically within and should be within the purview of the expertise of the standards drafting team. NRECA posits that the proposed SAR should clearly identify and support a reliability objective/risk that needs to be addressed and not propose specific requirement language. The SAR should identify the risk (the what) and the SDT should evaluate the alternatives for requirement language (the how) to address such a risk.

3. The SAR states that no other alternatives have been considered for addressing the reliability objectives.

4. As proposed in the SAR, the new reliability standards requirements would result in low impact BES Cyber Systems being subjected to more stringent communication security requirements than medium impact BES Cyber Systems are generally. Currently, only medium impact BES Cyber Systems at Control Centers are subject to CIP-005-6, R1.5. This scope of assets was determined by the standards drafting team responsible for those requirements after much analysis and deliberate effort. Given this clear, deliberate scoping of BES Cyber Systems relative to CIP-005-6, R1.5, NRECA respectfully asserts that the current SAR represents a conflict with previous risk assessments. In particular, if medium impact BES Cyber Systems generally were not considered as a risk for malicious communication, the inclusion of low impact BES Cyber Systems does not seem justified or justifiable. NRECA requests that NERC re-evaluate this and remove this inappropriate requirement for low impact BES Cyber Systems.

In summary, NRECA requests that this proposed SAR should be remanded back to the requester to address the above comments.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

PNM Resources agree with EEI comments.
Additionally, to maintain consistency throughout the standards the Detailed Description, (2) and (3), should be aligned with the language ultimately used in CIP-005-7 R3.1 and R3.2, "Vendor Initiated Remote Access."

Likes 0	
Dislikes 0	

Response

Guy V. Zito - Northeast Power Coordinating Council - 10

Answer	No

Document Name	RS--5-5-20--2020-03_Supply_Chain_LIR_SAR_Unoffical_Comment_Form_04032020.docx
Comment	

In the Industry Need, request replace “third party” with “vendor” for consistency with CIP-013.

In the Purpose / Goal, #1 is similar to CIP-005 Part 1.5 which is applicable to High / Medium Control Centers. Implementing Goal #1 would result in this requirement not applying to other Medium Impact assets while applying to High and Low. Next, we cannot find this concern as a recommendation in the study. So, we recommend removing Goal #1.

Goal #2 is similar to CIP-005 Part 2.4. Goal #3 is similar to CIP-005 Part 2.5. The corresponding Requirement 2 includes Technically Feasible Exception (TFE) language. If Goals #2 and #3 include TFE language, we do not believe the industry will achieve a desirable result. We recommend including a process for excluding communications based on capabilities without requiring a TFE.

CIP-005 Part 2.4 does not have the language “when initiated.” Recommend consistency with Part 2.4.

Project Scope says there are “recommendations” in the NERC Supply Chain Risk Assessment Report. That report makes only one recommendation. We request that the single recommendation be explicitly included in this Project Scope.

Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
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

(1) detect known or suspected malicious communications for both inbound and outbound communications;

Southern supports the recommendation for the detection of known or suspected malicious communications for both inbound and outbound communications. However, the scope of the communication should be limited to routable communications. In addition, the scope of detection of malicious communications should be compatible with the CIP-003 access models.

(2) determine when active vendor remote access sessions are initiated; and

Southern supports this recommendation and requests that the SAR provide the SDT the flexibility to introduce new NERC defined terms, as needed, for Vendor Remote Access or alternatively, Low Impact Vendor Remote Access.

(3) disable active vendor remote access when necessary.

Southern supports this recommendation and, aside from the above comments, does not have any additional comments at this time.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment

Only where remote electronic access connectivity exists.

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3,6	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Due to the high volume of assets containing low impact BES Cyber Systems and the need to review for compliance, we request the Implementation Period to be sufficient to support large organizations.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas agrees with adding certain policies for low impact BES Cyber Systems. Texas RE seeks clarification on whether CIP-013-1 will also be adjusted to include low impact BES Cyber Systems as an applicable system, in accordance with NERC's Supply Chain Risk Assessment. Texas RE recommends adding low impact BES Cyber Systems as an applicable system to CIP-013-1. Additionally, Texas RE recommends that the definition of CIP Senior Manager found in the NERC Glossary of Terms is updated to reflect the following change:	

*A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through **CIP-014**.* Lastly, Texas RE recommends that CIP-003-8 R1 Part 1.1 is also updated to address CIP-012, CIP-013, and CIP-014. Currently, sub-part 1.1.9 stops at declaring and responding to CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

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

Guy V. Zito - Northeast Power Coordinating Council - 10	
Answer	
Document Name	

Comment

Incorporating elements of CIP-005 and CIP-010 into CIP-003, when those High/Medium Requirements do not apply to Lows will create difficulty for verifying compliance. For example asset inventory, baseline configuration, patch management activities for Lows. How can the Entity demonstrate compliance for Lows?

The detection of malicious communications requirement is new. It does not tie back to the Supply Chain Standards. This new requirement will require IDS (Intrusion Detection Services). This is out of this scope.

Without the other layers of cyber security controls, the Entity may not realize they've been compromised.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	
Document Name	

Comment

NRECA continues to believe that NERC and the Regional Entities should undertake at least one year of supply chain standard audits for medium and high impact BES Cyber Systems (which are not even effective until October 1, 2020) before beginning work on supply chain standard requirements for low impact BES Cyber Systems.

This is particularly important when due consideration is given to the recent executive order and potential new regulatory schema/framework for all BES facilities and supporting systems. More specifically, with the recent U.S. President's issuance of a supply chain-focused executive order on "Securing the U.S. Bulk Power System," NRECA is concerned that there could be duplication of efforts relative to Supply Chain risk and risk mitigation. The executive order requires substantial actions relative to future and existing BES facilities and supporting systems and networks. At this time, the extent and scope of this new regulatory schema and framework is unknown and – as a result – conflicts could arise with both the existing supply chain reliability standards and future efforts such as this one. For this reason, while DOE works to develop final rules/regulations by September 28, 2020, this SAR should be delayed allowing time to consider the outcome from the executive order.

NRECA acknowledges the Board of Trustee's resolution to act on these issues; however, the changing regulatory environment since that resolution was passed must also be recognized and presents a significant complicating factor. Given the likely overlap and potential for conflict between the executive

order and NERC's development of supply chain standards, NRECA urges prudency and caution to ensure that efforts are neither duplicative nor conflicting. We look forward to working with NERC staff, industry and DOE to determine the best way forward.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1,3,5 - NPCC

Answer	
Document Name	

Comment

The Taunton Municipal Lighting Plant supports the comments submitted by Brian Evans-Mongeon of Utility Services, Inc.:

Entities are not required to have many of the components of a medium impact CIP compliance program such as: asset inventory, baseline configuration, patch management. The creation of low impact requirements based on the three goals listed in this SAR would be difficult, if not impossible to accomplish without also requiring, if only by inference, that these program components exist.

Concern about the detection of malicious communications requirement since it does not tie back to the Supply Chain Standards. This new requirement will require IDS (Intrusion Detection Services), which seems inconsistent with determination of low impact.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Since CIP-003 contains elements of CIP-004, CIP-005, CIP-006, CIP-008, and CIP-010, Texas RE recommends the drafting team consider simply listing "Low Impact BES Cyber Systems" in the applicability column of relevant requirements in CIP-004 through CIP-014. Otherwise, the requirements may be effectively duplicated when put in CIP-003.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	
Comment	

IESO supports the comments submitted by NPCC

Incorporating only some elements of CIP-005 into CIP-003, and not the other remaining elements will create difficulty for verifying compliance. Also, without other additional layers of cyber security controls, the Entity may not realize they've been compromised.

The detection of malicious communications requirement is new. It does not tie back to the Supply Chain Standards. This new requirement will require IDS (Intrusion Detection Services). This is out of this scope.

Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	

We appreciate the work that the NERC CIP Standards Drafting Teams are making to develop compliance requirements that improve reliability and security of the Bulk Electric System. We also understand that assets containing low impact BES Cyber Systems are important to protect from malicious activity. That said, the standards development path that low impact BES Cyber Systems are headed for is starting to match the requirements scope for High and Medium impact BES Cyber Systems. Low impact requirements were originally developed and added to CIP-003 to be flexible and less burdensome than the other CIP Standards requirements for High and Medium impact systems.

Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3,4,5,6	
Answer	
Document Name	
Comment	

The Standards Drafting Team shoul give consideration to active remote connections with “vendors” who are contracted to operate a facility, For example, a vendor operating a wind park for a utility from the vendor's control center. The utility is still the GO/GOP.

Likes 0	
Dislikes 0	

Response

Barry Jones - Western Area Power Administration - 9 - MRO,WECC

Answer	
Document Name	

Comment

The term “malicious communication” is a direct borrowing from CIP-005-5 R1.5 for high and medium impact BCS and is based on FERC Order 706 (FERC Order No. 706, Paragraphs 496-503). From a technical perspective, this translates into an entity’s ability to identify ingress/egress protocol traffic to a low BCS, detect and discern known malicious communications protocol packets from non-malicious communications protocol packets and provide a notification, alert or other action in order to “make known” to the entity the malicious protocol packet. This is an activity which is performed by a technology - an Intrusion Detection/Intrusion Prevention System – IDS/IPS and is not based in Policy as requested in the SAR. The inspection (and detection) of ingress/egress protocol traffic for malicious communications could occur at a procedure level, however the process would be manual, time and resource consuming, and have a high frequency of errors. It is therefore infeasible from a policy or process perspective.

Because the language establishes the same requirement at low impact sites as a high or medium impact rated BCS, it will require entities with low impact sites to acquire, install and manage IDS/IPS technologies at low impact sites. This is a significant cost to industry based on a perception of an “aggregate misuse of numerous low impact BCS.”

A recommended option would be to revise CIP-002-5.1 to identify aggregate low impact categorization locations within the criteria of Attachment 1. This would require an entity’s to identify and categorize the aggregate points of low impact sites which potentially are closer to medium than low. If the combined aggregate criteria meets the medium impact categorization rating, the entity will protect the aggregate site or system with security controls commensurate to the aggregate medium impact rating. This utilizes risk as a basis rather than an assumption that *all* low impact sites are an aggregated risk.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 3,4,5,6, Group Name NCPA

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
Thank you for the opportunity to provide comments.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Shannon Ferdinand - Capital Power Corporation (MRRE 80) - NA - Not Applicable - MRO,WECC,Texas RE,NPCC,SERC	
Answer	
Document Name	
Comment	
Emphasis should be given on any new requirements to leverage the significant work that low impact registered entities completed to comply with the CIP-003-7 & 8 focusing on refinement of those processes to reduce vulnerabilities of low impact BES Cyber Systems. Requiring major changes to existing systems greatly increases the timeframe for installation as well as the cost while ignoring incremental refinements that can have a more immediate effect.	

Because these requirements could have a significant impact on pre-existing commercial arrangements, and therefore, consistent with FPA section 215, we ask that the Standard Drafting Team be forward-looking in the sense that the Reliability Standard should not dictate the abrogation or re-negotiation of currently effective contracts with vendors, suppliers or other entities.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
The language for (2) and (3) needs to match what was defined for CIP005-6 R2 Part 2.4 and Part 2.5. This ensures that the standards are consistent for High, Medium, and Low impact BCS that all External Routable Connectivity. Otherwise the language is vague and will lead to ineffective standards.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	

Comment
San Miguel Electric Cooperative agrees with the comments submitted by Barry Lawson of NRECA.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - NAGF - 6 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	

Comment
Comments: Emphasis should be given on any new requirements to leverage the significant work that low impact registered entities completed to comply with the CIP-003-7 & 8 focusing on refinement of those processes to reduce vulnerabilities of low impact BES Cyber Systems. Requiring major changes to existing assets greatly increases the timeframe for installation as well as the cost while ignoring incremental refinements that can have a more immediate effect. Because these requirements could have a significant impact on pre-existing commercial arrangements, and therefore, consistent with FPA section 215, we ask that the Standard Drafting Team be forward-looking in the sense that the Reliability Standard should not dictate the abrogation or re-negotiation of currently effective contracts with vendors, suppliers or other entities.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	

Comment
By putting L-BCS subject to many new requirements (for L-BCS at least), the L-BCS inventory becomes an evidence. Responsible Entity must have one. Basically, the BES Cyber Systems should be inventoried. After that, the criteria’s application or not will decide in which category a given BCS is falling: High, Medium or Low. It will be easier to see if the BCS are well categorized and if we didn’t miss something (like a BCS).

By the version 5 of NERC CIP Standards, you did a great effort to reorganize well the requirements from versions 3 and 4. Please, keep the requirements well organized.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3,6	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	
There should be consideration of creating a new CIP Reliability Standard separating required plans and implementations for protecting assets containing low impact BCS from the current CIP-003 Security Management Controls standard. Current reporting options with the CIP-003 R2 CMEP	

activities does not adequately illustrate the extensive protections required, where gaps are identified through CMEP activities, and presents challenges for future growth of low impact protections. There may also be value in updating CIP-002 R1.3 to require a discrete list of low impact BES Cyber Systems. Maintaining an inventory of low impact BES Cyber Systems would mitigate potential risk of inadvertent vendor remote access remaining unprotected. In addition, CIP-003 R1 should be updated to reflect required policy topics for all currently enforceable CIP Reliability Standards (through CIP-014) with updates reflected in the definition of CIP Senior Manager (or just remove the reference to specific standards from the definition).

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	
Document Name	

Comment

The term "suspected malicious communcations" is slightly vague and could subject an entitiy to additional reporting that does not protect the BES. It may need to be reworded using NIST concepts, terms, and guidance rather than CIP-005 terms.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	
Document Name	

Comment

N/A	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Entities are not required to have many of the components of a medium impact CIP compliance program such as: asset inventory, baseline configuration, patch management. The creation of low impact requirements based on the three goals listed in this SAR would be difficult, if not impossible to accomplish without also requiring, if only by inference, that these program components exist. Concern about the detection of malicious communications requirement since it does not tie back to the Supply Chain Standards. This new requirement will require IDS (Intrusion Detection Services), which seems inconsistent with determination of low impact.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	
Document Name	
Comment	
Please clarify in the SAR that these new requirements would only apply to sites that allow remote access.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	

Comment
Reclamation recommends adding supply chain risk management requirements to CIP-003-8 or adding low impact BES Cyber Systems to the scope of the documented supply chain cyber security risk management plans required by CIP-013-2. If the required BCS protections are to be extended to include remote access, the standard(s) should require protections against supply chain risks associated with low impact BCS because remote access is more frequently used with low impact BCS. Reclamation also recommends that malicious code detection/protection capabilities do not specifically have to be performed by a perimeter device, but can be performed directly on the asset being connected to (i.e., the Windows host, etc.). If this protection can only be provided by the perimeter device, entities could be looking at significant infrastructure changes. If simply running malicious code protections on their host assets themselves, this would address the security concern. The requirement should indicate “per cyber asset capability.” Running malicious code protections on every conceivable asset is not technically possible; for example, it can’t be run on most PLCs, switches, etc. Reclamation recommends the SAR drafting team thoughtfully assess the cost impacts associated with this SAR to effect changes in a cost-effective manner. The SAR proposes a significant increase in the scope of the affected standards, which will have a substantial impact on affected entities and should not be taken without appropriate consideration. Prior to proposing additional modifications, Reclamation recommends each SDT take additional time to completely identify the scope of each Standard Authorization Request to account for future potential compliance issues. This will provide economic relief for entities by minimizing the costs associated with the planning and adjustments required to achieve compliance with frequently changing standard versions. NERC should foster a compliance environment that will allow entities to fully implement technical compliance with current standards before moving to subsequent versions. To minimize churn among standard versions, Reclamation recommends the SAR drafting team coordinate changes with other existing drafting teams for related standards; specifically, Project 2016-02 and Project 2019-03.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	

Comment
RF believes the above can be accomplished by making it additional to CIP-003-8 Attachment 1.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	
Document Name	

Comment
N&ST disagrees with the draft SAR's identification of Project 2019-02 BES Cyber Systems Information Access Management as a related standard or SAR that should be assessed for impact as a result of this proposed project. Neither existing nor proposed BES Cyber Systems Information access management requirements apply to assets containing Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment
"These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments". The term "malicious communication" is a direct borrowing from CIP-005-5 R1.5 for high and medium impact BCS and is based on FERC Order 706 (FERC Order No. 706, Paragraphs 496-503). From a technical perspective, this translates into an entity's ability to identify ingress/egress protocol traffic to a low BCS, detect and discern known malicious communications protocol packets from non-malicious communications protocol packets and provide a notification, alert or other action in order to "make known" to the entity the malicious protocol packet. This is an activity which is performed by a technology - an Intrusion Detection/Intrusion Prevention System – IDS/IPS and is not based in Policy as requested in the SAR. The inspection (and detection) of ingress/egress protocol traffic for malicious communications could occur at a procedure level, however the process would be manual, time and resource consuming, and have a high frequency of errors. It is therefore infeasible from a policy or process perspective. Because the language establishes the same requirement at low impact sites as a high or medium impact rated BCS, it will require entities with low impact sites to acquire, install and manage IDS/IPS technologies at low impact sites. This is a significant cost to industry based on a perception of an "aggregate misuse of numerous low impact BCS." An option would be to revise CIP-002-5.1 to include an aggregate low impact categorization criterion in Attachment 1 and identify the aggregate points of low impact sites. If the combined aggregate criteria meets the medium impact categorization rating, the entity may be required to protect the aggregate site or system with security controls commensurate to the medium impact rating.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	
Document Name	

Comment
IPL has no further comments.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment
Southern does not have any additional comments at this time.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6

Answer	
Document Name	

Comment
Rather than a new standard aimed at low impact assets, NERC should put out non-binding guidance to allow smaller utilities to implement protections within their budgetary and resourse limitations.

Likes 0	
Dislikes 0	

Response