Comment Report

Project Name:	2020-03 Supply Chain Low Impact Revisions (Draft 1)
Comment Period Start Date:	8/27/2021
Comment Period End Date:	10/11/2021
Associated Ballots:	2020-03 Supply Chain Low Impact Revisions CIP-003-X IN 1 ST

There were 82 sets of responses, including comments from approximately 193 different people from approximately 128 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution?

2. Is it clear that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations?

3. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems?

4. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

5. The SDT is proposing an 18-month implementation plan. Would this proposed timeframe give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

6. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	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,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric	1	SERC

						Cooperative, Inc.		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power, Inc.	1	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Chase Snuffer	Rayburn Electric Cooperative	3	Texas RE
					Susan Sosbe	Wabash Valley Power Association	3	RF
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	4	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Jodi Jensen	Western Area Power Administration - Upper Great	1,6	MRO

						Plains East (WAPA)		
					John Chang	Manitoba Hydro	1,3,6	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1,3,5	MRO
					Joe DePoorter	Madison Gas and Electric	4	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					Bill Shultz	Southern Company Generation	5	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	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
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
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
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
DTE Energy	patricia ireland	4		DTE Energy	Patricia Ireland	DTE Energy - Detroit Edison	4	RF
					Karie Barczak	DTE Energy - Detroit Edison Company	3	RF
					Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF

Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC

					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Scott Miller	Scott Miller		SERC	MEAG Power	Roger Brand	MEAG Power	3	SERC

					David Weekley	MEAG Power	1	SERC
					Steven Grego	MEAG Power	5	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
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC

					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC
Santee Cooper	Tommy Curtis	5		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC

1. Do you agree the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution?

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

Answer	No
Document Name	

Comment

BPA acknowledges NERC's concern regarding "aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System." [SAR, p. 1]

BPA agrees with the placement and language of CIP-003-X R1.2.6, as well as Attachment 1, Sections 6.1 and 6.3.

BPA votes Negative because Attachment 1, Section 6.2 introduces a higher compliance bar for Low sites than for Medium, creating confusion and implementation difficulties. BPA believes that neither the SAR nor NERC's Supply Chain Risk Assessment report* intended to require a higher bar for Low systems than already exist in M/H systems for the following reasons:

1) The Supply Chain report indicates a goal to bring Lows in line with existing M/H requirements: On p. 13 of the Supply Chain report, the summary of Q4 states that the numbers of respondents who do not apply the M/H requirements equally to their Low systems was "contrary to the expectation… that entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems." This points to an intent to copy existing M/H requirements, not add an additional requirement.

2) The SAR is inconsistent, mentioning detection of malicious communications separately from vendor access in the Purpose section, but merging them for “locations that allow vendor remote access” in the Description section.

If the SAR intended for the malicious code requirement to apply to vendor remote access, then Section 6.2 should specify “vendor remote access” to align with 6.1 and 6.3.

If the SAR intended for the malicious code requirement to apply to all remote access, then Section 6.2 belongs in CIP-003-X Attachment 1, Section 3.

However, since there is no equivalent requirement for medium impact BCS, nor any projects to expand CIP-005 R1.5 to all medium impact BCS, then Section 6.2 should be removed entirely to avoid this higher requirement for low impact BCS.

Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4, Group Name DTE Energy

Answer	No
Document Name	

Comment

DTE agrees with the placement and language of CIP-003-X R1.2.6

DTE votes Negative because Attachment 1, Section 6.2 introduces a higher compliance bar for Low sites than for Medium and High.

Further, DTE suggests that CIP-005 R2.4 and R2.5 be modified to include the expanded scope of Low sites under applicable systems.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends the SDT add the words “active,” “remote,” and “Interactive Remote Access” to Attachment 1 Sections 6 to align the language with CIP-005-6 R2 and use NERC-defined terms where possible. Section 6 should be moved and included within Attachment 1 Section 3 and not made into a new section and add “If technically feasible” to 6.2 to account for leagacy systems that are not capable of detecting known or suspected malicious communications for both inbound and outbound communications.

From: ”Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining vendor remote access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.”

To: “Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for identifying active vendor remote access sessions;

6.2 If technically feasible, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling active vendor remote access.”

The phrase “determining active vendor remote access sessions” is not clear. The Technical Rationale refers more specifically to ‘when sessions are initiated.

Reclamation also recommends adding “Vendor” to the NERC Glossary of Terms.

Vendor - Persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator

services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

Sect. 6.2, "Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications," is impractical. When CTG OEMs interrogate our DCSs for long-term service agreement purposes we verify the identity of the requestor and throw a switch to grant them access, but as they collect data it is not possible to identify and deter in real time any risky communications. Verifying that the requestor is an authorized representative of the OEM should be sufficient.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

While the language addresses the risk of malicious communication, the term “system-to-system access” is ambiguous. This term has been informally discussed on several webinars and other industry forums but lacks a formal definition in the Glossary of Terms, which leads to inconsistent application throughout the industry. NRG recommends either adding a formal definition for “system-to-system access” or issuing guidance that includes only system-to-system access that either makes changes to a BES Cyber System or transfers files or data to a BES Cyber System; monitoring-only system-to-sytem remote access should be excuded.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No

Document Name	
Comment	

The Midwest Reliability Organization NERC Standards Review Forum (MRO NSRF) thanks the Standard Drafting Team (SDT) for their work in drafting language in response to the NERC Board of Trustees (BOT) recommendations and approved Standards Authorization Request (SAR). While the MRO NSRF have some concerns with the proposed language, we agree with the general purpose of Project 2020-03 - Supply Chain Low Impact Revisions. The MRO NSRF acknowledges that a vendor remotely accessing low impact BES Cyber Systems poses security risks to the Bulk Electric System (BES) that must be mitigated. We feel that this first posting is very close to a final acceptable product and addressing our concerns with clarification of verbiage around a vendor's remote access and in detecting known or suspicious malicious communications will result in passing the next ballot.

Below are our concerns with vendor remote access and malicious communication mitigation:

The MRO NSRF has concerns with the use of the undefined term 'vendor remote access'. The use of this term or phrase continues to cause inconsistencies with interpretation across regions that often results in over-reach or misinterpretation that read only information sharing somehow constitutes access. The phrase 'vendor remote access' should be clarified and either be in the NERC Glossary of Terms, Implementation Guidance, Technical Rationale, or addressed in a CMEP Practice Guide. The SDT could also choose to rephrase the language in way that would exclude read-only sessions.

In Section 6 the SDT chose to include language "including interactive and system-to-system access." While the MRO NSRF understands the drafting team took language from CIP-005 R2.4 to maintain consistency, this also increased the scope from what was stated in both the SAR and NERC BOT recommendations. Was it the SDT's intention to do this and is it allowed within the scope of the approved SAR?

The MRO NSRF offers the following suggestion for requirement language for the SDT's consideration:

Attachment 1 Section 6 – Vendor Communications with BES Cyber Systems

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS for assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions (including software updates) of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining vendor remote access sessions;

6.2. Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications as vendor remote access sessions are occurring; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	
Comment	

While the language addresses the risk of malicious communication, the term “system-to-system access” is ambiguous. This term has been informally discussed on several webinars and other industry forums but lacks a formal definition in the Glossary of Terms, which leads to inconsistent application throughout the industry. NRG recommends either adding a formal definition for “system-to-system access” or issuing guidance that includes only system-to-system access that either makes changes to a BES Cyber System or transfers files or data to a BES Cyber System; monitoring-only system-to-sytem remote access should be excuded.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI believes the proposed technical requirements are reasonable and address the FERC directive; however, the technical requirements are electronic access controls. The SDT should consider including the following language in a new Attachment 1 Section 3 3.3:

3.3 Implement controls that monitor and restrict vendor remote access that:

3.3.1 Has one or more method(s) for determining vendor remote access sessions;
3.3.2 Has one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

3.3.3 Has one or more method(s) for disabling vendor remote access.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

In general, Dominion Energy supports the comments by EEI.

In addition, Section 6, subparts 6.1, 6.2 and 6.3 do not appear to fully align with the intended mitigations associated with the NERC Board of Trustees’ Resolution dated February 6, 2020. The introduction of the requirement that includes "detecting known or suspected malicious communications" for all low impact BES Cyber Syetems is more stringent than the current requirements for monitoring communications on higher risk "medium" impact BES

Cyber Systems. This more stringent requirement, by definition, lower risk assets does not appear to align with the NERC BOT intent to address the remote access risks for low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
No Texas RE agrees objectives #2 and #3 have been addressed in the proposed revisions. Texas RE is concerned, however, the language proposed in Attachment 1, Section 6 does not address objective #1, “detect known or suspected malicious communications for both inbound and outbound communications”. The proposed language in Attachment 1, Section 6 would require entities to “implement a process to mitigate risks associated **with vendor remote access**,” including “[h]aving one or more method(s) for detecting known or suspicious malicious communications for both inbound and outbound communications.” (CIP-003-X, Attachment 1, Section 6.) Texas RE is concerned that Section 6’s focus on vendor remote access does not capture the full range of malicious communications contemplated under the low impact guidance documents. In the event of a supply chain attack, malicious communications can occur whether or not a Responsible Entity has established an authorized channel for vendor communications. Additionally, in the event of a supply chain attack, malicious communications, such as compromised Cyber Assets attempting to communicate with a Command and Control server, can occur at locations where the Responsible Entity has deliberately not established channels for vendor remote access. Based on this perspective, therefore, Texas RE recommends that the SDT clarify that CIP-003 low impact monitoring obligations extend to **all** inbound and outbound network traffic to mitigate the risk of suspicious or malicious traffic going unnoticed, not just in situations of vendor remote access. Texas RE recommends moving the proposed language in Attachment 1, Section 6.2 to Section 3 (Electronic Access Controls) so it is clear malicious communication monitoring and detection method obligations apply to all communications, not simply vendor remote access communications.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No

Document Name	
Comment	
Malicious communications is not required at all medium impact BCS. It is only required to detect malicious communications at medium impact BCS at Control Centers. It is unreasonable to have low impact requirements that are more stringent than some medium impact. The measures section in Attachment 2 provides great examples; however, the measures go above and beyond some medium impact requirements.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
Malicious communications is not required at all medium impact BCS. It is only required to detect malicious communications at medium impact BCS at Control Centers. It is unreasonable to have low impact requirements that are more stringent than some medium impact. The measures section in Attachment 2 provides great examples; however, the measures go above and beyond some medium impact requirements.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Suggest interchanging the order of 6.2 and 6.3. 6.2 as is not specific to vendor remote access and it would be clearer to understand the security objectives. To ensure even less confussion consider moving 6.2 to Section 3. The SARs scope of '(1) detect known or suspected malicious communications for both inbound and outbound communications' is not specific to only vendor remote access, but all routable protocol.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	

Answer	No
Document Name	

Comment

The language proposed in CIP-003-X Attachment 1 Section 6 does not comprehensively address the risk of malicious communication and vendor remote access to low impact BES cyber systems with possible areas of improvement as follows:

- Context and usage of the term 'malicious communication' needs clarity and BC Hydro proposes to add a definition of the term 'malicious communication' in "NERC glossary of terms" to support the understanding
- Similarly BC Hydro proposes defining and adding term 'vendor remote access' to NERC glossary of terms
- Who and what is considered a 'vendor' also need to be defined in the glossary of terms for clarity and understanding
- The language used in Section 6.2 is referring to 'known or suspected malicious communications'. The use of word 'suspected' is quite open with respect to application and usage. Entities may have varied understanding and consideration of what is suspected and what is not. BC Hydro recommends adding clarity and provide examples of use cases and applicability to improve understanding and to better scope the requirements.

CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.2 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.2 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote acces's however this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5. BC Hydro recommends rewording or removing Section 6.2 completely.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Tacoma Power does not agree with the proposed language and suggests the following edits:

- Attachment 1, Section 6, replace the high level Section 6 language with “Section 6: **Vendor remote access**: Each Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:”
- Attachment 1, Section 6, Bullet 6.2, “Having one or more method(s) for **monitoring** known or suspected malicious **vendor remote** communications for both inbound and outbound communications; and”

Tacoma Power is also concerned that Bullet 6.2 institutes more stringent requirements for low impact BCS at substations or generation units than what is currently required under CIP-005 for similar medium impact assets. The requirement in CIP-003-X should be limited to detection of malicious communications for assets at control centers, in alignment with the scope of CIP-005.

Likes 0	

Dislikes 0	

Response

JT Kuehne - AEP - 6	
Answer	No
Document Name	

Comment

While AEP agrees with the overall sentiment of the proposed language in Attachment 1 Section 6, we believe it could be modified to provide a more clear understanding of how Responsible Entities are expected to comply. AEP recommends that additional language be included to specify that Section 6 subparts are only applicable to Entities that have implemented vendor remote access as part of their business process. Please see recommendations for language below.

Section 6: Vendor remote access: For low impact BES Cyber System(s) identified pursuant to CIP-002, Responsible Enties that have implemented vendor remote access shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) that include:

6.1 Having one or more method(s) for determining when vendor remote access sessions have been initiated;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	

Comment

Malicious communications (whatever that means) has no bearing on access and was not part of the NERC Low Impact report so why is it in this draft? If NERC wishes to address malicous code, it should do it in Systems Administration.

We do not support the use of meaningless phrases such as malicious communications to meet security objectives for compliance. There is a tendency to re-use these phrases by SDT's in an effort to seemingly make it easier to use them because they exist in other areas of the standards however that propoagates a continual mantra of applying something that could mean anything to anyone. Why not just use language for what we are trying to acheive? Another meaningless phrases is system-to-system.

Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy supports EEI comments. Additional analysis would be needed to review the data diode configurations at low impact locations.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
Acciona Energy does not agree with the language proposed in Attachment 1 Section 6. Vendor remote access is not a defined term. For this to be an effective requirement this term needs to either be defined in the NERC Glossary of Terms, defined within Attachment 1 Section 6 or a term that is defined in the NERC Glossary of Terms should be used in lieu of it, such as Interactive Remote Access (Please note IRA definition would require modification to apply to low impact). If the Standards Drafting Team (SDT) were to define vendor remote access, Acciona Energy would suggestion the following definition: Vendor Remote Access (VRA):	

Access by a vendor(s) of the Responsible Entity from a Cyber Asset outside the asset containing low impact BES Cyber System(s) that permits remote commands, control functions, software changes or firmware changes (e.g. 'write permissions') of BES Cyber Assets of the low impact BES Cyber System(s).

Using the aforementioned definition for VRA, Acciona Energy would suggest the following Section 6 language:

Section 6: Vendor Remote Access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with Vendor Remote Access to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining Vendor Remote Access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound Vendor Remote Access communications; and

6.3 Having one or more method(s) for disabling Vendor Remote Access.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institute's (EEI) response to Question 1.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO

Answer	No
Document Name	

Comment

MPC supports MRO NERC Standards Review Forum comments.

Likes 0	
Dislikes 0	

Response	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
It is difficult to determine if the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems without first defining what “vendor remote access” is. The use of the undefined term “vendor remote access” in CIP-003-9 will cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. The term "malicious communications" should be defined. Is this known malware or does it include any communications to or from an unknown ip address? Would we get penalized for not recognizing a zero day attack? The term "session" should be defined (and maybe "remote session" as well). Is this an active session or any session that is currently defined but inactive (as in through established firewall rules). Could we be penalized for not disabling inactive sessions in the event of an attack?	
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 recommends the following additions (**Bold**) to Attachment 1 Section 6, aligning the proposed language with the NERC Board resolution and CIP-005 R2.4 of the NERC Reliability Standards: *Section 6: Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with **active** vendor remote access (including **Interactive Remote Access** and system-to-system **remote** access) to low impact BES Cyber Systems that includes:* *6.1 Having one or more method(s) for determining **active** vendor remote access sessions;* *6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and* *6.3 Having one or more method(s) for disabling **active** vendor remote access.*	
Likes 0	
Dislikes 0	

Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
The NERC Board Resolution recommends that malicious communication and vendor remote access be dealt with individually rather than together as is done in the proposed standard revisions. Therefore, APPA does not agree that the language meets what is specified in the NERC Board Resolution.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA agrees with several other utility comments that the proposed language is more stringent and not consistent with NERC CIP High and Medium Assets.	
Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with and support EEI comments.	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	No
Document Name	
Comment	
The NERC Board Resolution recommends that malicious communication and vendor remote access be dealt with individually rather than together as is done in the proposed standard revisions. Therefore, FMPA does not agree that the language meets what is specified in the NERC Board Resolution.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
The NERC Board Resolution recommends that malicious communication and vendor remote access be dealt with individually rather than together as is done in the proposed standard revisions. Therefore, OUC does not agree that the language meets what is specified in the NERC Board Resolution.	
Likes 0	

Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	

Comment
Southern supports the comments submitted by EEI. In addition, we note Section 6 requires implementation of a process for all assets containing low impact BCS even if no such vendor remote access capability exists. In these instances, it requires methods to determine, detect, and disable a non-existent capability. We suggest the process and implementation of it be made conditional upon such access existing.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment
MISO supports the comments of the Midwest Reliability Organization NERC Standards Review Forum (MRO NSRF) and thanks the Standard Drafting Team (SDT) for their work in drafting language in response to the NERC Board of Trustees (BOT) recommendations and approved Standards Authorization Request (SAR). While the MRO NSRF have some concerns with the proposed language, we agree with the general purpose of Project 2020-03 - Supply Chain Low Impact Revisions. The MRO NSRF acknowledges that a vendor remotely accessing low impact BES Cyber Systems poses security risks to the Bulk Electric System (BES) that must be mitigated. We feel that this first posting is very close to a final acceptable product and addressing our concerns with clarification of verbiage around a vendor's remote access and in detecting known or suspicious malicious communications will result in passing the next ballot. Below are our concerns with vendor remote access and malicious communication mitigation: The MRO NSRF has concerns with the use of the undefined term 'vendor remote access'. The use of this term or phrase continues to cause inconsistencies with interpretation across regions that often results in over-reach or misinterpretation that read only information sharing somehow constitutes access. The phrase 'vendor remote access' should be clarified and either be in the NERC Glossary of Terms, Implementation Guidance, Technical Rationale, or addressed in a CMEP Practice Guide. The SDT could also choose to rephrase the language in way that would exclude read-only sessions. In Section 6 the SDT chose to include language "including interactive and system-to-system access." While the MRO NSRF understands the drafting team took language from CIP-005 R2.4 to maintain consistency, this also increased the scope from what was stated in both the SAR and NERC BOT recommendations. Was it the SDT's intention to do this and is it allowed within the scope of the approved SAR?

The MRO NSRF offers the following suggestion for requirement language for the SDT's consideration:

Attachment 1 Section 6 – Vendor Communications with BES Cyber Systems

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS for assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions (including software updates) of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining vendor remote access sessions;

6.2. Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications as vendor remote access sessions are occurring; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	2020-03_Supply_Chain_Lows_Unofficial_Comment_Form (FINAL).docx

Comment

The applicable resolution calls for additional levels of protection; however, the proposed language places an unduly high burden for low impact locations from a cost-effectiveness perspective. In particular, the proposed language effectively requires that the level of protection for low impact assets be effectively equivalent to the level of protection required to be applied to medium-impact assets. GSOC proposes that the standard revision include qualifications similar to those on the medium-impact assets such as limiting the scope to those assets with External Routable Connectivity as well as explicitly limiting the scope to routable protocols.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

OKGE supports EEI comments.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E agrees with the comments provided by the Edison Electric Institute (EEI) related to the use of the wording “vendor remote access”. Either make this a term in the NERC Glossary or modify Section 6 as indicted in the EEI comments to help in consistency across the industry.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

To clarify and remove ambiguity associated with the BOT recommendations, the term “vendor remote access” should be defined in the NERC Glossary rather than in an attachment to a Standard. Defining “vendor remote access” will ensure registered entities have a consistent understanding of the term in this and other Standards that may use the term.

As an alternative to defining “vendor remote access” in Section 6, EEI offers the following for consideration.

Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: *For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:*

*6.1 Having one or more method(s) for determining **when** vendor remote access sessions **have been initiated**;*

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications:

*6.3 Having one or more method(s) for disabling **active** vendor remote access **when necessary.***

In addition to the above comments, the proposed language in Section 6, part 6.2 is understood to add new requirements that appear to obligate entities to install IDS-like solutions for low impact BCS which is a higher bar than what is currently required for EAPs at Medium impact BCS with ERC. While it is unclear whether this was the NERC BOT's intent, such a requirement raises questions about CIP-005-6, Requirement R1, subpart 1.5.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC agrees with the EEI Comment Form response, specifically the idea of limiting the requirement to Interactive Remote Access	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State would like to see a definition of vendor remote access either in the Glossary of Terms, Technical Rationale or in the other guides such as the Implementation or the CMEP guides. There is too much misinterpretation surrounding vendor remote access. Tri-State also recommends adding additional language to the term system-to-system to eliminate ambiguity. Proposed language would read ("including interactive and system-to-system **with command-and-control capability access**) ...	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	

Answer	Yes
Document Name	
Comment	

SMUD agrees that the proposed language addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems, but believes that it would create less confusion for industry if the a “low impact asset” was referred to as a “low impact facility.” Using lower case asset versus upper case Asset has been a source of confusion since the low impact standards became effective.

SMUD does not believe that CIP-003 R2 Section 6 Part 6.2 belongs in section 6. This requirement may be better suited for Section 3, but should be changed to clearly reflect that the applicability is to vendor remote access (which is not in the current wording as part of Part 6.2). At a minimum, SMUD recommends changing the wording in Part 6.2: e.g.

“6.2 For vendor remote access, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and….”

Regional Entities could potentially interpret 6.2 to increase the scope to have one or more methods for detecting any malicious communications. This could increase the cost to implement and burden of proof to demonstrate compliance. SMUD would suggest adding “vendor remote access” to the requirement so that the scope is absolutely clear.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	Yes
Document Name	
Comment	

: It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	
Comment	

Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with adequacy of implementing and auditing. See response to question 6 for more details.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3

Answer	Yes
Document Name	

Comment

PNMR does not agree with industry partners and their recommendation to define "vendor remote access" within the requirements. This definition should be left to the utility.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	Yes
Document Name	

Comment

BHE thanks the SDT for their work on this project, and commends the team on their fidelity to the SAR. BHE agrees the language proposed in Attachment 1 Section 6 satisfies the NERC Board resolution, but proposes the following recommendations to maximize congruence:

{C}1.) Revise 6.1 to read: “Having one or more method(s) for determining when vendor remote access sessions have been initiated;”

{C}2.) Revise 6.3 to read: “Having one or more method(s) for disabling active vendor remote access when necessary.”

{C}3.) Remove the Section 6 parenthetical “(including interactive and system-to-system)” as it was not mentioned in the resolution, and could imply the same level of required protection as called for in CIP-005-7 R2.4 and R2.5, which may not be justified for low impact assets.

Instead, please address within the technical rationale document, Rationale Section 6 of Attachment 1, the intended scope of vendor remote access with respect to vendor read-only access for both system-to-system and interactive access. BHE proposes the last sentence, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	

Response

Brian Belger - Seattle City Light - 6

Answer	Yes
Document Name	

Comment

Yes, however, the use of the undefined term ‘vendor remote access’ continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for initiating and disabling a vendor’s ability to remotely perform command and control functions of the low impact BCS.

Additionally, regarding 6.2, while it is a good idea and certainly supports risk management of vendor remote access, this seems outside the scope of the vendor remote access section. Including it here implies that we should detect known or suspected malicious communications only within the context of vendor remote access sessions. To be more clear, we would suggest moving this sub requirement from 6.2 to instead become 3.3 within the electronic access controls section.

Moreover, there is a need to further clarify and define the term “vendor”. Does this exclude contractors and consultants?

There is no need to single out vendors when discussing remote access for whatever purpose. Any remote access, whether it be vendor, contractor, consultant, employee, engineer, programmer – they are all users employing remote access and as such, should be subject to security controls contemplated and spelled out in Attachment 1, Section 3 without having to be spelled out in minute detail. Although this section was designed for Supply Side Security, it could simply state that vendors are also subject to all security controls that other users are subject to when it comes to remote access. As such, preventive and corrective security controls/measures taken by the entity apply to them as well.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	Yes
Document Name	
Comment	

While N&ST agrees the proposed Section 6 requirements align well with the Board's 3-part resolution, N&ST believes they lack sufficient precision and clarity (e.g., would they apply to ANY vendor remote access to assets containing low impact BES Cyber Systems or only to those subject to "Electronic Access Controls" defined in CIP-003-8, Attachment 1, Section 3?).

Likes 0	
Dislikes 0	
Response	

Michael Jang - Seattle City Light - 1

Answer	Yes
Document Name	
Comment	

The use of the undefined term 'vendor remote access' continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for initiating and disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

Additionally, regarding 6.2, while it is a good idea and certainly supports risk management of vendor remote access, this seems outside the scope of the vendor remote access section. Including it here implies that we should detect known or suspected malicious communications only within the context of vendor remote access sessions. To be more clear, we would suggest moving this sub requirement from 6.2 to instead become 3.3 within the electronic access controls section.

Moreover, there is a need to further clarify and define the term "vendor". Does this exclude contractors and consultants?

There is no need to single out vendors when discussing remote access for whatever purpose. Any remote access, whether it be vendor, contractor, consultant, employee, engineer, programmer – they are all users employing remote access and as such, should be subject to security controls contemplated and spelled out in Attachment 1, Section 3 without having to be spelled out in minute detail. Although this section was designed for

Supply Side Security, it could simply state that vendors are also subject to all security controls that other users are subject to when it comes to remote access. As such, preventive and corrective security controls/measures taken by the entity apply to them as well.

Likes 0	
Dislikes 0	

Response

Scott Kinney - Avista - Avista Corporation - 3

Answer	Yes
Document Name	

Comment

It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	

Comment

It does address the risk, but as written it increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.

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 Regional Standards Committee

Answer	Yes
Document Name	

Comment

Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with the adequacy of implementing and auditing. See the response to question 6 for more details.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

CenterPoint Energy Indiana Electric (SIGE) agrees the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution.

Likes 0	
Dislikes 0	

Response

Hao Li - Seattle City Light - 4

Answer	Yes
Document Name	

Comment

Yes, however, the use of the undefined term ‘vendor remote access’ continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for initiating and disabling a vendor’s ability to remotely perform command and control functions of the low impact BCS.

Additionally, regarding 6.2, while it is a good idea and certainly supports risk management of vendor remote access, this seems outside the scope of the vendor remote access section. Including it here implies that we should detect known or suspected malicious communications only within the context of

vendor remote access sessions. To be more clear, we would suggest moving this sub requirement from 6.2 to instead become 3.3 within the electronic access controls section.

Moreover, there is a need to further clarify and define the term “vendor”. Does this exclude contractors and consultants?

There is no need to single out vendors when discussing remote access for whatever purpose. Any remote access, whether it be vendor, contractor, consultant, employee, engineer, programmer – they are all users employing remote access and as such, should be subject to security controls contemplated and spelled out in Attachment 1, Section 3 without having to be spelled out in minute detail. Although this section was designed for Supply Side Security, it could simply state that vendors are also subject to all security controls that other users are subject to when it comes to remote access. As such, preventive and corrective security controls/measures taken by the entity apply to them as well.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller

Answer	Yes
Document Name	

Comment

BHE thanks the SDT for their work on this project, and commends the team on their fidelity to the SAR. BHE agrees the language proposed in Attachment 1 Section 6 satisfies the NERC Board resolution, but proposes the following recommendations to maximize congruence:

1.) Revise 6.1 to read: “Having one or more method(s) for determining when vendor remote access sessions have been initiated;”

2.) Revise 6.3 to read: “Having one or more method(s) for disabling active vendor remote access when necessary.”

3.) Remove the Section 6 parenthetical “(including interactive and system-to-system)” as it was not mentioned in the resolution, and could imply the same level of required protection as called for in CIP-005-7 R2.4 and R2.5, which may not be justified for low impact assets.

4.) Instead, please address within the technical rationale document, Rationale Section 6 of Attachment 1, the intended scope of vendor remote access with respect to vendor read-only access for both system-to-system and interactive access. BHE proposes the last sentence, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	Yes

Document Name	
Comment	
CenterPoint Energy Houston Electric (CEHE) agrees the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
BHE thanks the SDT for their work on this project, and commends the team on their fidelity to the SAR. BHE agrees the language proposed in Attachment 1 Section 6 satisfies the NERC Board resolution, but proposes the following recommendations to maximize congruence: 1.) Revise 6.1 to read: “Having one or more method(s) for determining when vendor remote access sessions have been initiated;” 2.) Revise 6.3 to read: “Having one or more method(s) for disabling active vendor remote access when necessary.” 3.) Remove the Section 6 parenthetical “(including interactive and system-to-system)” as it was not mentioned in the resolution, and could imply the same level of required protection as called for in CIP-005-7 R2.4 and R2.5, which may not be justified for low impact assets. 4.) Instead, please address within the technical rationale document, Rationale Section 6 of Attachment 1, the intended scope of vendor remote access with respect to vendor read-only access for both system-to-system and interactive access. BHE proposes the last sentence, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Yes, however, the requirements for malicious communications at low impact are similar to that which already exists in the current enforceable versions of CIP-005-6 Requirement R1 Part 1.5, which is applicable to Electronic Access Points (EAPs) for High impact BES Cyber Systems (BCS) and EAPs for Medium impact BCS at Control Centers. The existing CIP-005-6 requirement do not apply to Medium Impact BCS with External Routable Connectivity (ERC). Was it the 2020-03 SDT's intention for this draft of the proposed low impact requirements for malicious communication to impose IDS-like solutions for low impact that are in fact a higher bar than what would currently be required for EAPs at Medium impact BCS with ERC?

Also, the use of the undefined term 'vendor remote access' continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, ATC requests consideration of alternative phrasing like but not limited to the following for Attachment 1 Section 6:, "***Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes: 6.1 Having one or more method(s) for determining vendor remote access sessions; 6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and 6.3 Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.***"

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	Yes
Document Name	

Comment

Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with adequacy of implementing and auditing. See response to question 6 for more details.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	Yes
Document Name	

Comment

Although the language addresses the NERC Board resolution, it goes too far placing compliance burden beyond requirements established for high and medium impact. Low impact requirements should match the reliability risk. This problem begins in Requirement R1. For medium and high impact, this

point is covered by the defined term Interactive Remote Access which clearly defines “remote access” and includes both vendor and Responsible Entity. For low impact, “vendor remote access” is not defined and allows too much audit subjective interpretation.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Is it clear that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations?

Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	

Vendor remote access can be confused with vendor access via Transient Cyber Asset connected to the Responsible Entity's local network to "remotely" connect to an asset containing low impact BES Cyber Systems (behind physical security controls). "Vendor remote access" must be defined to remove all subjective audit interpretation. Suggest the following: Vendor remote access: for remote routable protocol access originating outside the Responsible Entity's physical security controls for assets containing low impact BES Cyber System via an Internet Service Provider (ISP) from Cyber Assets used or owned by vendors, contractors or consultants…

Likes 0	
Dislikes 0	
Response	

Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	
Comment	

The lack of definition or clarification of the word "remote" might create confusion, please consider adding a definition, either in the NERC Glossary or a standard-specific definition.

The phrase "interactive access" is also confusing and should be further defined/clarified within this document, or a different phrase should be used.

Additionally, the term "mitigate" in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term "mitigate" in the requirement language; but only within the CIP-013 Purpose statement. This makes it appear that the Low Impact requirement is more stringent than the higher impact levels.

Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	

Comment
Request clarification on “remote” since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. “Remote” could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow use of CIP-003-8, reference model 3. Request clarification on “remote location.” The question includes “remote location” which is not defined. Is the generation switch yard a different location than the generator? Suggest that language be included to specify that remote means physically external to the site to be consistent with the CIP Low Impact protection framework and requirements for communications. Request consistent use of “Low Impact” or “low impact.” The term “mitigate” in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term “mitigate” in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	

Comment
ITC agrees with the EEI Comment Form response

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	No
Document Name	

Comment
Needs to be further clarified

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
The Board Resolution recommends 3 projects to be revised in the standard with respect to policies for low impact BES Cyber Systems, the second of which is to determine with active vendor remote access sessions are initiated. So it is not clear that Section 6 only addresses vendor access to low impact assets. It appears to also address malicious communications and disabling vendor remote access which the Board Resolution suggests should be dealt with in separate revisions.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree Attachment 1 Section 6 only addresses a vendor's access to low impact assets containing BES Cyber Systems. Part 6.2 does not explicitly refer to vendor remote access sessions similarly to Parts 6.1 and 6.3, which could allow an interpretation that having one or more method for detecting known or suspected malicious communications for both inbound and outbound communications should be applied broadly to all low impact assets, regardless of whether vendor remote access sessions are permitted or not. Furthermore, Part 6.2 is worded similarly to CIP-005 R1 Part 1.5, which is applicable to Electronic Access Points (EAPs) for high impact BES Cyber Systems and EAPs for medium impact BES Cyber Systems at Control Centers. The proposed 6.2 as worded would imply that Electronic Security Perimeters (ESPs) and EAPs are required for all low impact BES Cyber Systems, which would also exceed the requirements for medium impact BES Cyber Systems since CIP-005 R1 Part 1.5 is only applicable at medium impact BES Cyber Systems at Control Centers and is not applicable to generation resources or transmission substations.	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	No
Document Name	

Comment	
The Board Resolution recommends 3 projects to be revised in the standard with respect to policies for low impact BES Cyber Systems, the second of which is to determine with active vendor remote access sessions are initiated. So it is not clear that Section 6 only addresses vendor access to low impact assets. It appears to also address malicious communications and disabling vendor remote access which the Board Resolution suggests should be dealt with in separate revisions.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with and support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Hao Li - Seattle City Light - 4	
Answer	No
Document Name	
Comment	
: No. Unless the section 6 is revised with the redefined “Vendor Remote Access” in the comments of #1.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	

Comment
The Board Resolution recommends 3 projects to be revised in the standard with respect to policies for low impact BES Cyber Systems, the second of which is to determine with active vendor remote access sessions are initiated. So it is not clear that Section 6 only addresses vendor access to low impact assets. It appears to also address malicious communications and disabling vendor remote access which the Board Resolution suggests should be dealt with in separate revisions.

Likes 0	
Dislikes 0	

Response

Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper

Answer	No
Document Name	

Comment
In 6.1 we are required to have "...one or more method(s) for determining vendor remote access sessions." Determining what about them? that they are active or that they merely exist, whether or not they are active. In 6.2 I don't see the benefit of monitoring outbound communications for malicious communications when those communications are only outbound, as with a data diode. the only reason I can think of to monitor outbound communications is as an indicator of response to a remote command & control server. That would only make sense in a two-way communication. In 6.3 I believe that "...disabling vendor remote access" could be interpreted as disabling ALL vendor remote access if any remote access is seen to have malicious communications. If there are multiple sessions ongoing to multiple vendors (as well as employees) we could be found in violation for not shutting down all vendor sessions upon learning that one session is suspicious. In addition we would have to be able to determine which sessions are vendors in order to avoid shutting down employee sessions. Either that or just shut them all down. There is no mention of notifications or timeframe here. Sessions must be monitored but it follows that unless someone is notified in a timely fashion of malicious communications, nothing can be done in a reasonable period of time. And what is a reasonable period of time? A minute, an hour, a day? If we use logging as a method of monitoring, would a daily check of the logs be sufficient. I think we're at the mercy of the auditor on this but those with CIP-005 experience may have a better feel for how this could be implemented and what an auditor might expect.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The SDT has not defined “Vendor” to date. Without “vendor” being defined it is difficult to tell who would be in scope and required to adhere to Attachment 1 Section 6. This is also problematic in regards to Supply Chain for Medium Impact and High impact BES Cyber Systems. We would suggest defining “vendor”.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree Attachment 1 Section 6 only addresses vendor’s access to low impact assets containing BES Cyber Systems. Part 6.2 does not explicitly refer to vendor remote access sessions similarly to Parts 6.1 and 6.3 which could allow interpretation that having one or more method for detecting known or suspected malicious communications for both inbound and outbound communications should be applied broadly to all low impact assets, regardless of whether vendor remote access sessions are permitted or not.

Furthermore, Part 6.2 is worded similarly to CIP-005 R1 Part 1.5 which is applicable to Electronic Access Points (EAPs) for high impact BES Cyber Systems and EAPs for medium impact BES Cyber Systems at Control Centers. The proposed 6.2 as worded would imply that Electronic Security Perimeters (ESPs) and EAPs are required for all low impact BES Cyber Systems, which would also exceed the requirements for medium impact BES Cyber Systems since CIP-005 R1 Part 1.5 is only applicable at medium impact BES Cyber Systems at Control Centers and is not applicable to generation resources or transmission substations.

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 Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification on “remote” since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. “Remote” could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow the use of CIP-003-8, reference model 3.

Request clarification on “remote location.” The question includes “remote location” which is not defined. Is the generation switch yard a different location than the generator?

Request consistent use of “Low Impact” or “low impact.”

The term “mitigate” in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term “mitigate” in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
The language in Attachment 1, Section 6.2 – Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications is too broad if it is meant to only cover malicious communications relating to vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
The language in Attachment 1, Section 6.2 – Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications is too broad if it is meant to only cover malicious communications relating to vendor remote access.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	

To ensure complete clarity, Acciona Energy suggests using a defined term, please see Acciona Energy's answer to question 1.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

Request clarification on "remote" since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. "Remote" could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow use of CIP-003-8, reference model 3.

Request clarification on "remote location." The question includes "remote location" which is not defined. Is the generation switch yard a different location than the generator?

Request consistent use of "Low Impact" or "low impact."

The term "mitigate" in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term "mitigate" in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Request clarification on "remote location" with respect to BCS

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
The terminology of low impact BES cyber systems versus low impact assets needs to be clarified.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
It includes malicious communications which has nothing to do with access.	
Likes 0	
Dislikes 0	
Response	
Michael Jang - Seattle City Light - 1	
Answer	No
Document Name	
Comment	
Unless the section 6 is revised with the redefined “Vendor Remote Access” in the comments of #1.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	

Answer	No
Document Name	
Comment	

Tacoma Power does not agree that the proposed language clearly addresses vendor's access to low impact assets containing cyber systems from remote locations. Tacoma Power suggests the following edit to Attachment 1, Section 6, Bullet 6.2, "Having one or more method(s) for **monitoring** known or suspected malicious **vendor remote** communications for both inbound and outbound communications; and"

Tacoma Power is also concerned that Bullet 6.2 institutes more stringent requirements for low impact BCS at substations or generation units than what is currently required under CIP-005 for similar medium impact assets. The requirement in CIP-003-X should be limited to detection of malicious communications for assets at control centers, in alignment with the scope of CIP-005.

Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	
Comment	

As mentioned in comments related to Question 1 above, 'vendor remote access' needs clarity of understanding and clear definitions of the terms for appropriate applicability.

Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	
Comment	

N&ST believes the proposed Section needs to be clear about whether or not it applies only to BES assets containing low impact BES Cyber Systems that are subject to "Electronic Access Controls" defined in CIP-003-8, Attachment 1, Section 3.

Likes 0	
Dislikes 0	

Response	
Brian Belger - Seattle City Light - 6	
Answer	No
Document Name	
Comment	
No. Unless the section 6 is revised with the redefined “Vendor Remote Access” in the comments of #1.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Consider not using ‘a process’ in CIP-003, which is consistent with other Sections of CIP-003. The first part of Attachement 1 speaks to having plan(s). Also suggest using ‘electronic access controls’ as used in other Sections or just ‘controls.’ Consider the following edits for clarification: “Section 6: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002 that permit active vendor remote access to low impact BES Cyber Systems, the Responsible Entity shall implement electronic access controls to mitigate risks associated with active vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:” To be consistent with the language of the SAR and CIP-005-6, consider using ‘active vendor remote access’ and not just ‘vendor remote access’ in Section 6, 6.1 and 6.3. From a technical basis it is not clear what would the difference be between the two uses.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	

The way the 6.2 is written it appears that all communications must be monitored for malicious communication. It is not apparent that the malicious communications requirement only applies to situations where vendor remote access is allowed. This is only present in the technical rationale document, and it should be more clearly stated in CIP-003-X Attachment 1.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

The way the 6.2 is written it appears that all communications must be monitored for malicious communication. It is not apparent that the malicious communications requirement only applies to situations where vendor remote access is allowed. This is only present in the technical rationale document, and it should be more clearly stated in CIP-003-X Attachment 1.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

CIP-003 Section 6.2 requirement seems to establish a higher bar than the similar requirement in CIP-005 R1.5 for MIBCS at Control Centers. Additionally, CIP-003 R2 requirement establishes the applicability to “at least one asset identified in CIP-002 containing low impact BES Cyber Systems”. Why is it necessary to restate applicability in CIP-003 R2, Att1, Sec 6. Usage of this statement is inconsistently used through CIP-003 R2, Att1.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No

Document Name	
Comment	
In Attachment 1, Section 6, it is clear that the section is addressing vendor access to low impact assets containing BES cyber systems. However, it is not clear that the access is from remote geographical locations or from outside the point where electronic communication is controlled. Nowhere in Section 6 does it reference “remote locations”.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The IESO supports the NPCC submitted comments	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
In Attachment 1, Section 6, it is clear that the section is addressing vendor access to low impact assets containing BES cyber systems. However, it is not clear that the access is from remote geographical locations or from outside the point where electronic communication is controlled. Nowhere in Section 6 does it reference “remote locations”.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No

Document Name	
Comment	
Access from remote locations is not the same as remote access. A vendor could be physically on site and connect to the system through a remote connection.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Attachment 1, Sections 6.1 and 6.3 clearly specify that they apply to vendor access. BPA does not believe Section 6.2 provides the same clarity.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
The language in Attachment 1, Section 6.2 – Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications is too broad if it is meant to only cover malicious communications relating to vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	

Comment
Yes, but for additional clarity BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity's network is not considered vendor remote access.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	

Comment
PG&E agrees to the language in Section 6 only addresses vendor access to low impact assets containing BES Cyber Systems.

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
It is clear Section 6 only addresses vendor's access to assets containing low impact BES Cyber Systems from remote locations. However, in conjunction with EEI comments on Q1 further clarity on both 'remote' and 'access' is needed. For example, is data from an entity's BCS that is directed through a data diode to physically enforce an outbound only connection to a vendor system included in 'system-to-system vendor remote access'?

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes

Document Name	
Comment	
Yes, but for additional clarity BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity's network is not considered vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	

Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	

Yes, but for additional clarity BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity's network is not considered vendor remote access.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD would like to see more clarity regarding what constitutes a vendor. If an entity has contracted with an orgization to operate an asset, are all communications and connections from outside of the asset considered vendor remote access? There are use cases where the entity may contract the operation of an asset that the entity itself has no access to.

Would a contractor, issued an entity provided/managed laptop, working from an entity owned facility, that has been onboarded using the same process as all entity employees that have been granted unescorted and electronic access still be considered a vendor?

The two examples provided are use cases that SMUD feels should not be left up to the region entities.

Likes 2	Platte River Power Authority, 5, Archie Tyson; DTE Energy, 4, ireland patricia
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	Yes
Document Name	
Comment	
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	

3. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems?

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The IESO Supports the NPCC Submitted comments

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

In general, Dominion Energy supports the comments from EEI.

In addition, Dominion Energy is concerned that when reviewing Attachment 1, Section 6 the current language appears to broaden the scope of applicability to any asset containing the low impact BES Cyber Systems rather than just to the low impact BES Cyber System itself. The language should be clarified to enure that the scope is limitied to just the cyber system and not the entire asset.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

Current low impact BCS do not include or required IDS/IPS. The proposed revisions seem to expand the need for them.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	

Comment
Current low impact BCS do not include or require IDS/IPS. The proposed revisions seem to expand the need for them.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	

Comment
Section 6 includes “vendor remote access” which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include “vendor remote access”. This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3. Recommend adding “vendor remote access sessions” to 6.2. For example, “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and” For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed. Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – “Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers.” Another possibility is to leverage CIP-003 Section 3 “Electronic Access Control” scoping / boundary language. CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5’s Requirement but R1.5 is applicable to High Impact EAP’s and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5’s Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.

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 Regional Standards Committee	
Answer	No
Document Name	
Comment	

Section 6 includes “vendor remote access” which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include “vendor remote access”. This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3.

Recommend adding “vendor remote access sessions” to 6.2. For example, “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and”

For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed.

Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – “Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers.” Another possibility is to leverage CIP-003 Section 3 “Electronic Access Control” scoping / boundary language.

CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5’s Requirement but R1.5 is applicable to High Impact EAP’s and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5’s Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

The language in Sections 6.1-6.3 applies to assets that contain BES Cyber Systems. This potentially draws in remote access to non-CIP devices that are located within that asset. The language should be updated to specifically point to the BES Cyber System within the low impact asset. This is different than the way that CIP-003 is written and may need a different Requirement to address.

Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	
Comment	
We agree with and support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC agrees with the EEI Comment Form response	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Section 6 includes “vendor remote access” which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include “vendor remote access”. This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3. Recommend adding “vendor remote access sessions” to 6.2. For example “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and” For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed. Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – “Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers.” Another possibility is to leverage CIP-003 Section 3 “Electronic Access Control” scoping / boundary language.	

CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5's Requirement but R1.5 is applicable to High Impact EAP's and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5's Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1

Answer	No
Document Name	

Comment

Section 6 includes "vendor remote access" which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include "vendor remote access". This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3.

Recommend adding "vendor remote access sessions" to 6.2. For example, "Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and"{C}{C}

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No
Document Name	

Comment

Language exceeds medium and high impact by not exempting low impact BES cyber systems not having External Routable Communication. This increases scope.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3

Answer	Yes

Document Name	
Comment	
CIP-003 R2 requirement establishes the applicability to “at least one asset identified in CIP-002 containing low impact BES Cyber Systems”. Why is it necessary to restate applicability in CIP-003 R2, Att1, Sec 6. Usage of this statement is inconsistently used through CIP-003 R2, Att1.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
While it does limit the scope to low impact BES cyber systems, it does not limit the scope to only those **assets** containing low impact BES cyber systems that permit vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Brian Belger - Seattle City Light - 6	
Answer	Yes
Document Name	
Comment	
However, the use of the term ‘vendor remote access’ continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for: **Attachment 1 Section 6:,** **Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:** **6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;**	

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

We also request consideration of alternative language in the parent requirement such as: Requirement "**R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS**".

Likes 0	
Dislikes 0	

Response

Michael Jang - Seattle City Light - 1

Answer	Yes
Document Name	

Comment

The use of the term 'vendor remote access' continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:,

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

We also request consideration of alternative language in the parent requirement such as: Requirement "***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***".

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	Yes
Document Name	
Comment	
It does because CIP-003 is applicable only to Low Impact assets (not Cyber Systems)	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
The language implies that additional analysis is required for vendor remote access once an analysis was performed.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	

Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	

Yes, NERC Reliability Standard CIP-003-8, Attachment 1 is only applicable to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

SIGE agrees the language in Attachement 1 Section 6 limits the scope to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

The NAGF has no comments.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	Yes
Document Name	

Comment

APPA suggests deleting the lead-in of, “Vendor remote access: .” Otherwise, the first clause of the sentence in Section 6 limits the scope to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	
Hao Li - Seattle City Light - 4	
Answer	Yes
Document Name	
Comment	

However, the use of the term ‘vendor remote access’ continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:,

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for disabling a vendor’s ability to remotely perform command and control functions of the low impact BCS.

We also request consideration of alternative language in the parent requirement such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”.

Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	Yes
Document Name	
Comment	

FMPA suggests deleting the lead-in of, “Vendor remote access: .” Otherwise, the first clause of the sentence in Section 6 limits the scope to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	Yes
Document Name	

Comment

OUC suggests deleting the lead-in of, “Vendor remote access: .” Otherwise, the first clause of the sentence in Section 6 limits the scope to low impact BES Cyber Systems.

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 believes the language in CIP-003 R2 makes it clear that all sections in Attachment 1 are limited in scope to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E believes the language of Section 6 limits the scope to low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
However, the use of the term ‘vendor remote access’ continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, ATC requests consideration of alternative phrasing like but not limited to the following for Attachment 1 Section 6:, “***Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact***	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
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	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

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	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cost can vary widely depending on interpretation of vague language.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Applying section 6 to facilities containing low impact BES may require significant costs in hardware (Firewall upgrades) or additional out of band circuits, etc.) to be able to detect and disable VRA at remote and/or unmanned locations.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
At this point, we believe the framework still requires significant modifications before assessing the cost effectiveness of the proposal.	
Likes 0	
Dislikes 0	

Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE expects Section 6.2 implementation to require additional technology and resources over and above Section 3 requirements. The concern is with the supply chain timelines and physical implementation across a great many assets containing low impact BES Cyber Assets. The large scope will take time to implement and may also require a significant monetary expenditure. While the SDT cannot do anything to mitigate costs, the implementation timeline can be expanded to allow for what will be a project of greater scope than any similar projects affecting only medium and high impact BES Cyber Assets.	
Likes 0	
Dislikes 0	

Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC does not agree with the EEI response. ITC believes that this requirement is NOT as cost effective and would require specialized equipment and/or processes.	
Likes 0	
Dislikes 0	

Response	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	No
Document Name	
Comment	
Additional consideration needs to be given to the Virtualization project and flexibility that access approach can allow	
Likes 0	

Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment
At this time PG&E does not have information to determine if the modifications are a cost-effective approach. PG&E would have preferred to answer this as un-known and not “No”, but that option does not exist within the NERC Standards Balloting and Commenting System (SBS).

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment
Due to the number of assets potentially affected by the proposed changes as well as the complexity of the proposed measures, implementation of proposed language would be disproportionately costly to implement given the risks associated with low-impact assets. GSOC proposes that the standard revision include qualifications similar to those on the medium-impact assets such as limiting the scope to those assets with External Routable Connectivity as well as explicitly limiting the scope to routable protocols

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

MISO supports the comments submitted by the MRO NSRF and does not believe that the modifications are cost effective within the confines of the current implementation plan. The implementation of security measures for vendor remote access at the vast amount of assets containing LIBCS, often remotely located, would be highly impactful to entities' budgets and may require a phased-in approach to spread costs over several fiscal years.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

This question is very utility specific; for some smaller utilities this may be more difficult and costly to implement than it would be for larger utilities. This brings into question if the risk that the smaller utilities presents is commensurate with the increased expenditure.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller

Answer	No
Document Name	

Comment

BHE expects Section 6.2 implementation to require additional technology and resources over and above Section 3 requirements. The concern is with the supply chain timelines and physical implementation across a great many assets containing low impact BES Cyber Assets. The large scope will take time to implement and may also require a significant monetary expenditure. While the SDT cannot do anything to mitigate costs, the implementation timeline can be expanded to allow for what will be a project of greater scope than any similar projects affecting only medium and high impact BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	
Comment	
NCPA does not agree it's cost effective for Low Impact Assets to be subjective to more stringent requirements than NERC CIP High and Medium impact Assets.	
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 cost and implementation could be quite significant if entities were to have to renegotiate contracts and put in place remote vendor access controls for remote low-impact facilities The cost to achieve compliance with Attachment 1, Section 6.2 at low impact locations, which goes above and beyond medium and high location requirements, may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Low impact environments are often unmanned and lack the types of infrastructure required for determining, detecting, and disabling malicious activity (IDS, IPS, SEIM, Intermediate Systems, etc…). These new requirements could potentially expand the scope of existing low impact programs with respect to cost for new monitoring functionality.	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	No
Document Name	
Comment	
MPC supports MRO NERC Standards Review Forum comments.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
The changes as written in Section 6.2 would require implementation of equipment/processes for monitoring communications at each Low Impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy does not believe that the modifications will be cost effective within the current scope of the implementation plan. The cost of deploying security measures to meet the requirements within an 18 month time frame at hundreds of low impact substations and other assets will be a strain on entities budgets and existing IT/OT security personnel. Evergy suggests spreading this effort out across a longer time frame of 36 months or more to be less impactful financially and more realistically achievable.	
Likes 0	
Dislikes 0	
Response	

Scott Kinney - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
The changes as written in Section 6.2 would require implementation of equipment/processes for monitoring communications at each Low Impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Many entity's will believe that "malicious communications" translates to Intrusion Detection Systems for Low Impact assets. That could translate to $millions for entity's.	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power recommends editing the language in Attachment 1, Section 6, Bullet 6.2 in order to provide a more cost effective approach. Instead of detecting, Tacoma Power proposes changing the measure to monitoring for malicious vendor remote access communication, as follows: Attachment 1, Section 6, Bullet 6.2, “Having one or more method(s) for **monitoring** known or suspected malicious **vendor remote** communications for both inbound and outbound communications; and”	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Although the cost may differ between entities, it's impact may change based on understanding & clarity of terms and scope of application. As advised in comments of Question 1 above, CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. However requirement in CIP-003-X Section 6.2 applies to 'Low Impact BCS' which is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5 where only High and Medium Impact BCS at Control Centers are in scope leaving all the other Medium impact BCS. Implementing this requirement and adding detection methods for known or suspected malicious communications for both inbound and outbound communications concerning Low impact BCS will likely have significant cost impact	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes that a considerable amount of research would be needed before many respondents would be able to provide a well-informed answer to this question. We note that the December 2019 “Supply Chain Risk Assessment” report states, “More than 99% of the responders (to a survey question about costs and benefits) agreed with the draft response that it was premature for CIP-013 registered entities to determine or estimate costs or benefits	

associated with the implementation of the standard…" That said, N&ST believes the cost to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
BHE expects Section 6.2 implementation to require additional technology and resources over and above Section 3 requirements. The concern is with the supply chain timelines and physical implementation across a great many assets containing low impact BES Cyber Assets. The large scope will take time to implement and may also require a significant monetary expenditure. While the SDT cannot do anything to mitigate costs, the implementation timeline can be expanded to allow for what will be a project of greater scope than any similar projects affecting only medium and high impact BES Cyber Assets.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
If current procedural controls are not sufficient to achieve compliance, then there will be additional costs. Additional licensing that is expensive may be required. Where is there sufficient risk to warrant the increase in cost?	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	

Comment	
If current procedural controls are not sufficient to achieve compliance, then there will be additional costs. Additional licensing that is expensive may be required. Where is there sufficient risk to warrant the increase in cost?	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The broad scope of the proposed language appears to bring all low impact assets into scope as it requires all communication to all assets be monitored at alkl times for malicious communication through vendor remote access, whether the access is being utilized or not.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Until the technical issues referenced in response to questions 1 and 2 are addressed, the cost effectiveness of the approach to compliance cannot accurately be determined.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
The MRO NSRF does not believe that the modifications are cost effective within the confines of the current implementation plan. The implementation of security measures for vendor remote access at the vast amount of assets containing LIBCS, often remotely located, would be highly impactful to entities' budgets and may require a phased-in approach to spread costs over several fiscal years.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	

Comment
Until the technical issues referenced in response to questions 1 and 2 are addressed, the cost-effectiveness of the approach to compliance cannot accurately be determined.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	

Comment
Sect. 6.2, "Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications," is impractical. When CTG OEMs interrogate our DCSs for long-term service agreement purposes we verify the identity of the requestor and throw a switch to grant them access, but as they collect data it is not possible to identify and deter in real time any risky communications. Verifying that the requestor is an authorized representative of the OEM should be sufficient.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No

Document Name	
Comment	
Reclamation identifies that it is not cost effective to have separate standards for low impact and medium impact BES Cyber Systems, especially when the language of the requirements for each impact level is identical. Reclamation observes that Project 2016-02 will bring many changes to a majority of the CIP standards; therefore, Reclamation recommends this project may be a good avenue to incorporate low impact requirements into these standards to avoid the continuous churn of CIP-003 Attachment 1 when ultimately the requirements for low impact BES Cyber Systems will end up being identical to those for medium impact BCS.	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	No
Document Name	
Comment	
The cost and implementation could be quite significant if entities were to have to renegotiate contracts and get access to assets for which they are registered for, but that they do not have access to. Cost to achieve compliance with Attachment 1, Section 6.2 at low impact locations, which goes above and beyond medium and high location requirements, may not be cost effective	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA does not believe that adding an additional requirement to Low systems over current M/H requirements is cost effective.	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
The changes as written in Section 6.2 would require implementation of equipment/processes for monitoring communications at each Low Impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	
Given the ambiguity around what constitutes “vendor remote access” it is difficult to determine what it would take to comply with the proposed requirements or determine if the modifications would be cost effective. Would a contractor that is issued an entity provided/managed laptop, working from an entity owned facility, that has been onboarded using the same process as all entity employees that have been granted unescorted and electronic access still be considered a vendor? The cost and implementation could be quite significant if entities were to have to renegotiate contracts and get access to assets for which they are registered for, but that they do not have access to.	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
TMLP believes that the cost of implementing these additional protections will not be overly burdensome in the sense of adding equipment, but the time that it takes to complete small daily/regular tasks may be increased and therefore may increase labor expenses.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE agrees the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports the MRO NSRF’s comments for Question 4.	
Likes 0	
Dislikes 0	
Response	

Michael Jang - Seattle City Light - 1	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP agrees that the proposed modifications are cost-effective so long as a couple criteria are met: • The proposed language AEP has suggested in response to Question #1 is incorporated in Attached 1 Section 6. Proving the negative is burdensome to the Responsible Entity, and the proposed language will ensure Responsible Entites are not required to do so should they not have vendor remote access implemented as part of their business process. Please see AEP's response to Question #1 above. • The solution to meet the vendor remote access requirements can be implemented at the network or perimeter level rather than at the device or substationlevel.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
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	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hao Li - Seattle City Light - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Belger - Seattle City Light - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	
Document Name	
Comment	
This question is very utility specific; for some smaller utilities this may be more difficult and costly to implement than it would be for larger utilities. This brings into question if the risk that the smaller utilities presents is commensurate with the increased expenditure.	
Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
This question is very utility specific; for some smaller utilities this may be more difficult and costly to implement than it would be for larger utilities. This brings into question if the risk that the smaller utilities presents is commensurate with the increased expenditure.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing an 18-month implementation plan. Would this proposed timeframe give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month Implementation Plan. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel/vendors appropriately.	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
We do not believe that the technology exists to identify and deter in real time any risky communications by the OEM when interrogating the DCS, nor is it likely to become available in the next eighteen months.	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The IESO supports the NPCC submitted comments.	
Likes 0	
Dislikes 0	

Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The implementation of security measures, such as IDS/IPS, for vendor remote access at a vast amount of assets containing LIBCS would be impactful to entities' budgets and may require a phased-in approach over 36 months to spread costs over different fiscal years. The phased-in approach could have an initial effective date begin at 18 months for Sections 6.1 and 6.3 and conclude with full implementation of 6.2 at 36 months.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI recommends a 24-month impelemntation plan given the large vendor solution diversity within a very non-homogenous array of low-impact facilties. Entities may need to compile a inventory of applicable Cyber Assets to determine the impact of the proposed requirements as entities are currently not required to maintain a discrete listing of Cyber Assets at low impact facilities, which are most likely to contain multiple vendor solutions. This extended implementation plan provides entities sufficient time to conduct an inventory of applicable BCAs and BCSs, and implement additional electronic access controls which may be both procedural and technical in nature.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy generally supports EEI comments. A minimum 36 month implementation period, based on the current broad scope of the proposed standard impacting DERs, which are rarely manned but have remote access for operations, would be necessary to design, install, and train for new equipment and capabilities.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

An entity that has high and medium impact BCS in addition to low impact facilities would have an easier time implementing these requirements; however, an entity that is only low impact would have a challenging time meeting this the 18-month implementation timeframe. At least a 24-month timeframe should be considered.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

An entity that has high and medium impact BCS in addition to low impact facilities would have an easier time implementing these requirements; however, an entity that is only low impact would have a challenging time meeting this the 18-month implementation timeframe. At least a 24-month timeframe should be considered.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment	
BHE does not agree that 18 months is adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to compile detailed lists of low impact BES Cyber Assets and vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess and document remote access at all of their affected facilities, which is not an inconsequential task. For these reasons, the implementation plan should be on the order of 24 to 36 months.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes the time, effort, and cost to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3. N&ST recommends a 24 month implementation time frame.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro recommends a longer implementation plan e.g. ~ 36 months considering the cost and scope impact as identified in comments of Question 4 and 1 above. Once the clarity of terms and definitions as identified per our comments to Questions 1 and 4 is obtained, BC Hyrdo will be in a better position to provide an alternate detailed implementation plan to meet the target completion deadline.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	No
Document Name	
Comment	
The requirement to review and affect changes need a longer duration to implement. An implementation plan of a minimum of 36 months to complete the changes. A significant amount of prerequisite work must be done in order to come into compliance with the proposed requirements.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Recommend a 24-month implementation	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	

Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
We suggest 24 months because of the number of assets with low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	

Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institute's (EEI) response to Question 5.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree the proposed timeframe provides enough time to put into place process, procedures, or technology to meet the proposed language in Section 6. Some entities have a higher number of low impact systems than medium or high impact systems, therefore deploying technology to these locations will take much more time.	
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 Regional Standards Committee	
Answer	No
Document Name	
Comment	

Recommend a 24-month implementation due to the significant scale of Low Impact.

As written, some entities may opt for compliance over security and operational reliability. Based on the scope of the requirement, the scale of BES Assets, and the proposed 18-month implementation time, it appears Responsible Entities would be incentivized to not utilize or disconnect technology solutions to avoid compliance risks. Avoiding compliance risks may result in Responsible Entities reducing capabilities that support reliability or security functions, such as managed (security and operational) support and response functions.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO

Answer	No
Document Name	

Comment

MPC supports MRO NERC Standards Review Forum comments.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

With most entities budgeting 18-24 months in advance, for new infrastructure and staffing resources, this could be a problematic timeline. The Entity would need to update their processes, procedures, train staff, hire resources, and implement technology. All this would need to be completed once budget has been approved. Based on Entity budgeting and the multiple items that will need to be address we would suggest 24-36 months.

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 recommends that the proposed implementation plan be modified to allow for 24-36 months following the effective date. This timeframe will allow entities to implement the necessary hardware/software, procedural, and vendor contract changes at low impact facilities.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See comment provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA suggests that 24 months be given for implementation to procure, configure, install, train and write procedures associated with the task of detecting malicious communication.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	

Answer	No
Document Name	
Comment	
Presently, there is no requirement obligating a "low" asset list. We believe that these changes would require compiling a detailed list. In our opinion because we have a vast amount of low Cyber Systems, 18 months would not be adequate time to compile and validate such a list.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	No
Document Name	
Comment	
BHE does not agree that 18 months is adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to compile detailed lists of low impact BES Cyber Assets and vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess and document remote access at all of their affected facilities, which is not an inconsequential task. For these reasons, the implementation plan should be on the order of 24 to 36 months.	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS feels that a 24-month implementation plan would be a reasonable timeframe to implement process, procedures or technology to meet the proposed language in Section 6. It may be necessary to design and implement multiple solutions to meet the proposed language in Section 6 across the various environments in which low impact assets are in use. Alternatively, a single solution which could be applied across a broader group of low assets may require significant design changes to process, procedures and/or technology.	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree the proposed timeframe provides enough time to put into place process, procedures, or technology to meet the proposed language in Section 6. Some entities have a higher number of low impact systems than medium or high impact systems, therefore deploying technology to these locations may take much more time. CEHE recommends a 36-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO supports comments submitted by the MRO NSRF. The implementation of security measures, such as IDS/IPS, for vendor remote access at a vast amount of assets containing LIBCS would be impactful to entities' budgets and may require a phased-in approach over 36 months to spread costs over different fiscal years. The phased-in approach could have an initial effective date begin at 18 months for Sections 6.1 and 6.3 and conclude with full implementation of 6.2 at 36 months.	
Likes 0	
Dislikes 0	

Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Due to the number of assets potentially affected by the proposed changes and high likelihood that additional technical controls will need to be implemented, 18 months would not be adequate to implement the proposed measures. To allow for budgetary allocation and implementation for technical measures needed to comply with the proposed changes, GSOC recommends a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
OKGE supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
18 months is not adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to implement substantial new protections for low impact BES Cyber Assets in order to monitor and control vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess & document vendor-specific remote access at all of their affected facilities, which is a significant undertaking. Given the current supply chain issues/delays underscores the substantial and impacts on entities' ability to timely secure materials necessary to implement these changes. For these reasons, the implementation plan should be a minimum of 36 months.	

In addition, Attachment 1, Section 6, part 6.2 could be understood to require entities to install IDS-like solutions for low impact BCS. Given the large number of locations and the efforts that will be required to implement 6.2 and the aforementioned supply chain delays, 36 months is more than reasonable . While a phased approach may be another solution, the logistics of effectively implementing a phased approach will be difficult to both budget, administer and audit.	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	No
Document Name	
Comment	
Additional time of 24 months due to potential funding cycles needed for implementation	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE does not agree that 18 months is adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to compile detailed lists of low impact BES Cyber Assets and vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess and document remote access at all of their affected facilities, which is not an inconsequential task. For these reasons, the implementation plan should be on the order of 24 to 36 months.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	

Comment
Recommend a 24-month implementation due to the significant scale of Low Impact. As written, some entities may opt for compliance over security and operational reliability. Based on the scope of the requirement, the scale of BES Assets, and the proposed 18-month implementation time, it appears Responsible Entities would be incentivized to not utilize or disconnect technology solutions to avoid compliance risks. Avoiding compliance risks may result in Responsible Entities reducing capabilities that support reliability or security functions, such as managed (security and operational) support and response functions.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment
If the scope is clear, 18-months for implementation should be fine. Given some of the ambiguity in the current draft, more specifically, the lack of clarity of key terms, it is difficult to determine the extent of changes or what additional technical resources necessary to comply. Additionally, some entities may have very limited security technologies in place for or at low impact assets that can be re-used for the purpose of meeting the requirements. For those entities, it may take much more time to architect, procure, and deploy a solution. Given the potentially large number of low impact sites, 18-months could be challenging.

Likes 0	
Dislikes 0	

Response

Brian Belger - Seattle City Light - 6

Answer	Yes
Document Name	

Comment
Instead of an 18-month plan, an implementation plan could be broken down to a few phases, which each phase has its milestones. This approach will allow small entities with no resources to find ways to implement gradually while large entities with more resources may implement all in once.

Likes 0	
Dislikes 0	

Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP believes the 18-month implementation plan allows for enough time so long as: • the requirement is applicable to Responsible Enties that have implemented vendor remote access as noted in the response to Question #1, and • the solution to meet the vendor remote access requirements can be implemented at the network-level rather than at the device-level as noted in our response to Question #4. Should that not be the case, a 36-month implementation plan would be more appropriate.	
Likes 0	
Dislikes 0	
Response	
Michael Jang - Seattle City Light - 1	
Answer	Yes
Document Name	
Comment	
Instead of an 18-month plan, an implementation plan could be broken down to a few phases, which each phase has its milestones. This approach will allow small entities with no resources to find ways to implement gradually while large entities with more resources may implement all in once	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports the MRO NSRF’s comments for Question 5.	
Likes 0	
Dislikes 0	

Response	
Hao Li - Seattle City Light - 4	
Answer	Yes
Document Name	
Comment	
Instead of an 18-month plan, an implementation plan could be broken down to a few phases, which each phase has its milestones. This approach will allow small entities with no resources to find ways to implement gradually while large entities with more resources may implement all in once.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E believes the 18-mont implementation plan can be achieved base on our current setup but understands the concerns raised in the EEI comments related to supply chain delays for other entities and would be willing to support a 36-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Our specific system will not have a problem trying to meet an 18-month implementation plan, but we do have some concerns for the entire Low Impact category due to the large amount of entities who fall under this category, and the varying degree of size and abilities of the entities who fall under this category. Some entities may be less equipped to handle these issues than others.	
Likes 0	

Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
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	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	
Document Name	
Comment	
Unable to comment on this.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	

Tri-State does not agree with an 18-month implementation plan. Again, applying section 6 to facilities containing low impact BES may require significant costs in hardware (Firewall upgrades) or additional out of band circuits, etc.) to be able to detect and disable VRA at remote and/or unmanned locations. A longer phased-in approach would be more appropriate for planning and budgeting purposes. Tri-State suggests a 36 month phased-in approach.

Likes 0	
Dislikes 0	

Response

6. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.	
Russell Noble - Cowlitz County PUD - 3	
Answer	
Document Name	
Comment	
I also support comments provided by Utility Services.	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	
Document Name	
Comment	
TMLP believes that it may be necessary to require the vendor provide the Registered Entity with logging information about who and what was done during the remote session. While we recognize that this was listed as one of the options in the CIP-003-X Attachment 2 for Section 6, we believe that this should be required in some manner.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	
Document Name	
Comment	
1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access.	

a. “Remote” would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA.

b. VRA needs to be limited to access to BCS.

c. VRA must allow the use of CIP-003-8, reference model 3.

2) There are a number of issues with the CIP-003-X Technical Rationale

a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access.

b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find “3rd party” in the CIP-013 documents.

c. Where is the rest of the old “Guidelines and Technical Basis (GTB)?” We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models.

3) 6.1 - 6.3 are required even if the entity does not allow vendor remote access. It seems that the entity would have to perform these functions for unauthorized vendor remote access if that can even exist.

a. The technical rational (TR) for 6.2 states: “The obligation in Section 6.2 requires that entities which allow vendor remote access.” We request updating the Requirement by adding “vendor remote access.” To be consistent with 6.1 and 6.3.

4) Request consistent language between 6.1 / 6.3 and CIP-005-6 R2.4 / R2.5. 6.1 and 6.3 are almost the same as CIP-005-6 R2.4 and R2.5 but R2.4 and R2.5 uses the phrase “active vendor remote access sessions”. 6.1 and 6.3 do not include the word “active”. Without the word ‘active’, 6.1 and 6.3 could include or maybe be limited to “capability” of the vendor or the BES configuration and electronic access controls.

a. The TR for 6.1 uses “that are taking place” and the TR for 6.3 uses “active”. Sections 6.1, 6.3 and the TR should consistently use the word “active”.

b. R2.4 and 2.5 are only applicable to High Impact and Medium Impact with ERC. Both include PCA’s. This makes Low Impact more stringent than Medium Impact (non-ERC).

5) As written in 6.2, Lows will be a higher bar than Medium which seems to be in contrast to the intent of current CIP Standards risk-based approach (High – Medium – Low). CIP Standards start in CIP-002 with system and asset categorization that establishes a risk-based approach (impact levels) as per the bright line criteria with controls commensurate of the risk (impact levels). There is no corresponding requirement for non-Control Center, Medium Impact. This makes Low Impact more stringent than Medium Impact (non-Control Center).

6) Request the retention of the Guideline and Technical Basis. It appears that some information is moved to the proposed Technical Rationale. But the diagrams and their explanations seem to be struck out of CIP-003 and not moved elsewhere. Request clarification – will the CIP-003-8 reference models continue to be valid?

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	
Document Name	

Comment
The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. ATC requests the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements. Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. ATC requests consideration of alternative language such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”. Carry this concept through to Attachment 1 Section 6.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	

Comment
As mentioned in Q1, BHE wishes the technical rationale document to address the intended scope of vendor remote access with respect to vendor read-only access. BHE would not expect vendor read-only access, which could be used for health monitoring, to be a risk requiring Section 6 protective measures. BHE proposes the the last sentence of Rationale Section 6 of Attachment 1, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows. BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity’s network is not considered vendor remote access.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	

ITC prefers to retain the Technical Rationale, especially verbiage that limits scope to Low Impact and Interactive Remote Access.

Furthermore, ITC believes this requirement is not as cost effective as mentioned by EEI. In Section 6.2 a requirement to scan traffic for suspicious, malicious communication requires specialized equipment and/or processes. Today, this is only necessary under CIP-005-6 R1.5 for High Impact. The impression is that we're talking about skipping Medium and going to Low. This does not appear to follow a risk based approach.

Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

EEI also notes that the SDT did not request comment on the modifications to Requirement 1, subpart 1.2 which is material to the draft. In the modifications to this section, we note that the SDT has used the undefined term “vendor remote access”, while leveraging this key term in both Requirement 1, subpart 1.2.6 and Attachment 1, Section 6 even though this term is not well understood by the industry. EEI recommends defining of this term. (See our comments to Question 1)

Additionally, EEI believes it may be more efficient and effective over time to simply reference all parts of Attachment 1 within Requirement 1, subpart 1.2 rather than modifying Requirement 1 each time changes are made to the requirements associated with CIP-002, containing low impact BES Cyber Systems.

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	

We would like to thank the SDT for preparing the changes and allowing us to comment. We do have a concern not addressed by the above questions:

While the revisions address the risk of malicious communications outlined by the NERC Board resolution, this is NOT a requirement for medium impact BES Cyber Systems not at Control Centers. This was brought up by ACES at the final CIPC meeting as CIP-005 R1.5's applicable systems are high impact and medium impact BES Cyber Systems at Control Centers. This creates more stringent controls for low impact BCS, than medium impact BCS which we object to. While this new requirement was part of the NERC study low impact BCS should not have to meet greater requirements than higher impact level BCS.

Further, there is not an existing project to change CIP-005 R1.5 to include all medium impact BCS and the CIP-005 revision from Project 2016-02 do not change the Applicable Systems to include medium impact BCS not at Control Centers. Without adding medium impact BCS to CIP-005 or removal of this proposed requirement, the standards will leave a gap for medium impact BCS not at a Control Center when considering malicious communications.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	
Document Name	

Comment

PG&E has no additional comments on the modifications.

Likes 0	
Dislikes 0	

Response

Sarosh Muncherji - British Columbia Utilities Commission - 9

Answer	
Document Name	

Comment

There is the usual direct supply chain where specific vendor products are utilized for BES cyber system operations and maintenance. There are other sources of software that may possibly be overlooked as being part of the "supply chain" and these products may slip through the cracks. Examples include freeware utilities such as text editors (for example, NotePad++) and communications programs (for example, PuTTY). The SDT may consider requiring software integraty validation for all software in a future revision to the standard.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	
Document Name	

Comment

Of significant note, the proposed changes do not reference protecting only a routable communication medium, leaving the language unclear as it relates to non-routable connections as might be found in low-impact field equipment. Similar requirements in medium-impact systems are only required at Control Centers as reflected in CIP-005 R1.5 or are otherwise qualified based on the connectivity of the cyber asset, e.g., CIP-005-6, R2.4, R2.5. Thus, the proposed requirements for low-impact assets require greater protections across a larger swath of assets than the ones governing medium-impact assets. The proposed language, therefore, raises the protections of low-impact assets to that of high-impact assets, thereby removing any risk-based differentiation of controls between impact ratings.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	
Document Name	

Comment

Section 6, items 1-3 appear to try and address the 3 separate Board Resolution recommendations as vendor remote access. Each should be addressed separately to ensure revision clarity. As stated above in the answers to questions 1&2 the language is not specific. Is this for detection methods for all inbound and/or outbound communications? For example, if you use a data diode, would you still need to detail a method for monitoring all inbound and outbound malicious communications?

Likes 0	
Dislikes 0	

Response

LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman

Answer	

Document Name	
Comment	
Section 6, items 1-3 appear to try and address the 3 separate Board Resolution recommendations as vendor remote access. Each should be addressed separately to ensure revision clarity. As stated above in the answers to questions 1&2 the language is not specific. Is this for detection methods for all inbound and/or outbound communications? For example, if you use a data diode, would you still need to detail a method for monitoring all inbound and outbound malicious communications?	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	
Document Name	
Comment	
As mentioned in Q1, BHE wishes the technical rationale document to address the intended scope of vendor remote access with respect to vendor read-only access. BHE would not expect vendor read-only access, which could be used for health monitoring, to be a risk requiring Section 6 protective measures. BHE proposes the the last sentence of Rationale Section 6 of Attachment 1, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows. BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity’s network is not considered vendor remote access.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	

We request that the Guidelines and Technical Basis are not removed from the standard. The Technical Rationale document released with these changes only addresses the new Section 6 changes, and does not replace the comprehensive Guidelines and Technical Basis currently in the standard. The current Guidelines and Technical Basis are used as reference documentation by NERC Regional Entities and Generator Owners, and we believe have played a critical role in the development of compliance programs and internal controls.

Likes 0	
Dislikes 0	

Response

Hao Li - Seattle City Light - 4

Answer	
Document Name	

Comment

The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. We request the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements.

Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. We request consideration of alternative language such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”. Carry this concept through to Attachment 1 Section 6 to remove “vendor remote access” from use in CIP-003-X.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

Comments: Section 6, items 1-3 appear to try and address the 3 separate Board Resolution recommendations as vendor remote access. Each should be addressed separately to ensure revision clarity. As stated above in the answers to questions 1&2 the language is not specific. Is this for detection methods for all inbound and/or outbound communications? For example, if you use a data diode, would you still need to detail a method for monitoring all inbound and outbound malicious communications?

Likes 0	
Dislikes 0	

Response
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker
Answer
Document Name
Comment
See comment provided by EEI.
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 supports preserving the language identified for deletion in Section 6 – Background and Attachment 2 – Guidelines and Technical Basis (GTB).
Likes 0
Dislikes 0
Response
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3
Answer
Document Name
Comment
We believe that requirements for controlling remote access are adequately addressed by Section 3: Electronic Access Controls, and therefore find the proposed Section 6 unnecessary.
Likes 0
Dislikes 0

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	
Document Name	

Comment
When the CIP-005 R2.4-2.5 requirements were added, entities were able to leverage existing monitoring systems and infrastructure in their High and Medium Impact Control and Data Center environments (IDS, IPS, SEIM, Intermediate Systems, etc…). Additionally, with remote Medium Impact sites, entities were already required to institute use of an Intermediate System for IRA. For assets containing Low Impact BES Cyber Systems, typically unmanned and with fewer applicable requirements, this type of infrastructure is often not in place. With the high volume of Low Impact sites, this could pose an enormous and untenable burden on RE's.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO

Answer	
Document Name	

Comment
MPC has no additional comments.

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 Regional Standards Committee

Answer	
Document Name	

Comment
1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access.

a. “Remote” would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA.

b. VRA needs to be limited to access to BCS.

c. VRA must allow the use of CIP-003-8, reference model 3.

2) There are a number of issues with the CIP-003-X Technical Rationale

a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access.

b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find “3rd party” in the CIP-013 documents.

c. Where is the rest of the old “Guidelines and Technical Basis (GTB)?” We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	
Document Name	

Comment

SIGE would like additional clarity within the technical rationale as to whether virtual meeting sessions (e.g. such WebEx or Zoom meetings where the screen is shared, either escorted or unescorted) are considered vendor remote sessions.

Additionally, “asset” needs to be defined within the NERC Glossary of Term. “Asset” can be interpreted in many ways which may lead to inconsistent application of the requirements or definitions it is used in.

Likes 0	
Dislikes 0	

Response

Aric Root - CMS Energy - Consumers Energy Company - 4

Answer	
Document Name	

Comment
We believe that requirements for controlling remote access are adequately addressed by Section 3: Electronic Access Controls, and therefore find the proposed Section 6 unnecessary.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5	
Answer	
Document Name	

Comment
Exelon has chosen to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6	
Answer	
Document Name	

Comment
Exelon has chosen to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5	
Answer	
Document Name	

Comment

Acciona Energy has no additional comments at this time, thank you for your consideration.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	
Document Name	

Comment

1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access.

a. "Remote" would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA.

b. VRA needs to be limited to access to BCS.

c. VRA must allow the use of CIP-003-8, reference model 3.

2) There are a number of issues with the CIP-003-X Technical Rationale

a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access.

b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find "3rd party" in the CIP-013 documents.

c. Where is the rest of the old "Guidelines and Technical Basis (GTB)?" We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models.

3) 6.1 - 6.3 are required even if the entity does not allow vendor remote access. It seems that the entity would have to perform these functions for unauthorized vendor remote access if that can even exist.

a. The technical rational (TR) for 6.2 states: "The obligation in Section 6.2 requires that entities which allow vendor remote access." We request updating the Requirement by adding "vendor remote access." To be consistent with 6.1 and 6.3.

4) Request consistent language between 6.1 / 6.3 and CIP-005-6 R2.4 / R2.5. 6.1 and 6.3 are almost the same as CIP-005-6 R2.4 and R2.5 but R2.4 and R2.5 uses the phrase "active vendor remote access sessions". 6.1 and 6.3 do not include the word "active". Without the word 'active', 6.1 and 6.3 could include or maybe be limited to "capability" of the vendor or the BES configuration and electronic access controls.

a. The TR for 6.1 uses “that are taking place” and the TR for 6.3 uses “active”. Sections 6.1, 6.3 and the TR should consistently use the word “active”.

b. R2.4 and 2.5 are only applicable to High Impact and Medium Impact with ERC. Both include PCA’s. This makes Low Impact more stringent than Medium Impact (non-ERC).

5) As written in 6.2, Lows will be a higher bar than Medium which seems to be in contrast to the intent of current CIP Standards risk-based approach (High – Medium – Low). CIP Standards start in CIP-002 with system and asset categorization that establishes a risk-based approach (impact levels) as per the bright line criteria with controls commensurate of the risk (impact levels). There is no corresponding requirement for non-Control Center, Medium Impact. This makes Low Impact more stringent than Medium Impact (non-Control Center).

6) Request the retention of the Guideline and Technical Basis. It appears that some information is moved to the proposed Technical Rationale. But the diagrams and their explanations seem to be struck out of CIP-003 and not moved elsewhere. Request clarification – will the CIP-003-8 reference models continue to be valid?

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon has chosen to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon has chosen to align with EEI in response to this question.

Likes 0	

Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
Vendor remote access (VRA) is not a defined term Request clarification on “malicious communications” In case there is no “vendor remote access”, which evidence is to be produced ?	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy has a higher volume of low impact locations as compared to high or mediums. A significant amount of prerequisite work must be done in order to come into compliance with the proposed requirements.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	

Recommend the SDT address the term "system-to-system" by looking at CIP-002. This would greatly help industry by removing a meaningless phrase and helping industry by providing them a way to parse systems owned and used by vendors, systems owned by entity's but used by vendors, and/or systems owned and used by entities for remote access.

Recommend the SDT look at CIP-004 R4 to authorize vendors because it would align the concept of authorized vendors within the existing authorization standards and then only the systems used for access would need to be addressed in CIP-002 (recommendation 1)

Likes 0	
Dislikes 0	

Response

Michael Jang - Seattle City Light - 1

Answer	
Document Name	

Comment

The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. We request the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements.

Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. We request consideration of alternative language such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”. Carry this concept through to Attachment 1 Section 6 to remove “vendor remote access” from use in CIP-003-X.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	
Document Name	

Comment

No additional comments. AEP would like to express thanks to the standard drafting team’s hard work on this project.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	
Document Name	

Comment

Tacoma Power recommends clarifying that Attachment 2, Section 6 applies to vendor's access to low impact assets containing BES cyber systems from remote locations, as follows:

- Attachment 2, Section 6, Bullet 2: "2. Documentation of configuration of security alerts; security alerts or logging relative to activities during the **vendor remote** communication from items such as:"
- Attachment 2, Section 6: "**Vendor Remote Access:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:"

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	
Document Name	

Comment

BC Hydro ackowledges the effort and hard work by SDT which went into putting together these complex changes to CIP-003-X. As identified in comments to Question 1 and 4 above, the definitions of terms and clarity of application with some specific industry use case examples will provide a clear understanding and will help to get a faster and appropriate approvals of these proposed changes.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	
Document Name	

Comment

N&ST has reviewed the January 2020 NERC Member Representatives Committee “Policy Input Package” that preceded the February NERC Board meeting, and it is our principal observation that there was not a strong consensus among the members about the best approach to address concerns about coordinated attacks on low impact assets with vendor remote electronic access as the primary attack vector. We also noted that there were several suggestions to the effect that more comprehensive cost-benefit analyses should be performed before extending the scope of Supply Chain requirements to include low impact assets containing BES Cyber Systems.

N&ST notes the proposed requirement to require malicious communications detection at low impact assets containing BES Cyber Systems would, if effected, result in a more stringent requirement being imposed on low impact assets than on medium impact BES Cyber Systems with External Routable Connectivity at facilities other than Control Centers. N&ST is aware that the December 2091 NERC “Supply Chain Risk Assessment” raised the specter of coordinated, common mode attacks on large numbers of low impact assets, stating, “This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System.” While we acknowledge this possibility and agree it is of some concern, it is our opinion that it may make more sense, and achieve a better return on investment, to add a malicious communications detection requirement for medium impact first.

It is N&ST’s opinion that introducing the concept of lower-case “interactive” vendor remote access to BES Cyber Systems at low impact assets will cause needless confusion among entities subject to requirements for upper-case Interactive Remote Access, and therefore we recommend that it be dropped. We see no need to distinguish “interactive” vendor remote access from “system-to-system” vendor remote access in CIP-003.

Likes 0	
Dislikes 0	

Response

Brian Belger - Seattle City Light - 6

Answer	
Document Name	

Comment

The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. We request the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements.

Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. We request consideration of alternative language such as: Requirement “**R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS**”. Carry this concept through to Attachment 1 Section 6 to remove “vendor remote access” from use in CIP-003-X

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	
Document Name	

Comment

This includes systems used by vendors for system-to-system remote access and vendor "Interactive Remote Access (IRA)" (delete words in quotes) interactive remote access to low impact BES Cyber Systems.

Reasoning: The NERC defined term Interactive Remote Access includes the Electronic Security Perimeter, which is not a concept in CIP-003-8. Suggest using lowercase interactive remote access as is used in Attachment 1 Section 6 Part 6.1 – Determining Vendor Remote Access section of the document.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	
Document Name	

Comment

As mentioned in Q1, BHE wishes the technical rationale document to address the intended scope of vendor remote access with respect to vendor read-only access. BHE would not expect vendor read-only access, which could be used for health monitoring, to be a risk requiring Section 6 protective measures.

BHE proposes the the last sentence of Rationale Section 6 of Attachment 1, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.

BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity’s network is not considered vendor remote access.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	
Document Name	

Comment

Nothing additional at this time.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE has the following additional recommendations for the SDT:

- Include language for (1) software integrity and authenticity, (2) info system planning and (3) vendor risk and procurement controls, which addresses various aspects of supply chain risk management as is consistent with Reliability Standards CIP-013 and CIP-010.
- Include vendor multi-factor authentication (MFA). Passwords can be subjected to numerous cyber-attacks, including brute force. MFA provides an additional layer of security and protects systems should passwords become known by unauthorized users.
- Include controls for encrypted vendor remote access sessions, which is consistent with CIP-005 Requirement R2.

Texas RE also notes that the language proposed in Attachment 1, Section 6 utilizes the undefined term “interactive” in context to vendor remote access rather than the NERC defined term Interactive Remote Access (IRA). Since the current IRA definition is associated with ESPs, Texas RE would strongly

encourage revising the IRA definition to include “assets that contain low impact BES Cyber Systems.” The definition of IRA would read: “User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s ***assets that contain low impact BES Cyber Systems***, Electronic Security Perimeter(s), or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.”

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3

Answer	
Document Name	

Comment

PNMR believes there are substatial improvements to be made to provide clarity and consistency, not only within CIP-003 but also with CIP-005

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	

Comment

Attachement 2 Section 6 containes many capitalized terms that are not contained in the NERC glossary of terms. The SDT should consider not capitalizing the following terms: Security Information Management, Firewall, Intrusion Detection System, Intrusion Prevention System, Virtual Private Network, Remote Desktop, Removing, and Ethernet. By doing such the draft CIP-003-X Standard will further align with the usage of similar terms within the existing FERC approved CIP Standards.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	

Document Name	
Comment	
Please reference responses to questions 1 and 2.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The MRO NSRF has no additional comments at this time.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Our main concern was for our market participants. The proposed addition of 6.2 for "malicious communications detection" is infrastructure dependant and could prove difficult for low impact facilities without the necessary supporting infrastructure. While we accept the reasoning for it's proposed inclusion, we would prefer "6.2 Having one or more method(s) for detecting known or suspected malicious *communications for both inbound and outbound communications, per communications capability "* *Due to the large size and scope of any implementation, in particular for the proposed 6.2 requirement of "detect malicious communications", we would prefer to see a 24 month implementation period in order to allow enough time for entities to have a full budgeting and implementation cycle.*	
Likes 0	
Dislikes 0	

Response
Martin Sidor - NRG - NRG Energy, Inc. - 6
Answer	
Document Name	
Comment
Please reference responses to questions 1 and 2.
Likes 0	
Dislikes 0	
Response
Kevin Lyons - Central Iowa Power Cooperative - 1
Answer	
Document Name	
Comment
While the revisions address the risk of malicious communications outlined by the NERC Board resolution, this is NOT a requirement for medium impact BES Cyber Systems not at Control Centers. This was brought up by ACES at the final CIPC meeting as CIP-005 R1.5's applicable systems are high impact and medium impact BES Cyber Systems at Control Centers. The revisions being made to CIP-003-X create more stringent controls for low impact BCS than are currently required for medium impact BCS. While this new requirement was part of the NERC study, low impact BCS should not have to meet greater requirements than higher impact level BCS. Our position is that the same revisions should be made for medium impact BCS, whether through additional work in this project or through another project. Thank you for the opportunity to comment.
Likes 0	
Dislikes 0	
Response
Richard Jackson - U.S. Bureau of Reclamation - 1,5
Answer	
Document Name	
Comment

Reclamation recommends once virtualization/zero trust architecture is implemented the SDT start focusing on incorporating low impact requirements into the other standards where applicable and change the applicable systems of the other standards to include low impact BCS.

Reclamation appreciates the SDT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the SDT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	
Document Name	

Comment

This Standard brings in some medium/high impact requirements for low impact. The proposed language brings in a subset of the CIP-005 requirements, which creates more stringent controls for low impact BCS than medium impact.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF

Answer	
Document Name	

Comment

We believe that requirements for controlling remote access are adequately addressed by Section 3: Electronic Access Controls, and therefore find the proposed Section 6 unnecessary.

Likes 1	DTE Energy, 4, ireland patricia
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	
Document Name	

Comment	
NA.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	
Document Name	
Comment	
Definitions for Vendor remote access and what constitutes malicious communications would provide some clarity and help entities determine the cost effectiveness standard. SMUD suggests changing lower case “asset” to “facility” to remove the confusion that already exists. Moving requirement 6.2 to section 3 might make it more consistent with CIP-005.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
AEPCO has signed on to the ACES comments below: We would like to thank the SDT for preparing the changes and allowing us to comment. We do have a concern not addressed by the above questions: While the revisions address the risk of malicious communications outlined by the NERC Board resolution, this is NOT a requirement for medium impact BES Cyber Systems not at Control Centers. This was brought up by ACES at the final CIPC meeting as CIP-005 R1.5’s applicable systems are high impact and medium impact BES Cyber Systems at Control Centers. This creates more stringent controls for low impact BCS, than medium impact BCS	

which we object to. While this new requirement was part of the NERC study low impact BCS should not have to meet greater requirements than higher impact level BCS.

Further, there is not an existing project to change CIP-005 R1.5 to include all medium impact BCS and the CIP-005 revision from Project 2016-02 do not change the Applicable Systems to include medium impact BCS not at Control Centers. Without adding medium impact BCS to CIP-005 or removal of this proposed requirement, the standards will leave a gap for medium impact BCS not at a Control Center when considering malicious communications.

Likes 0	
Dislikes 0	

Response