

## Consideration of Comments

<b>Project Name:</b>	2020-03 Supply Chain Low Impact Revisions (Draft 2)
<b>Comment Period Start Date:</b>	2/25/2022
<b>Comment Period End Date:</b>	4/15/2022
<b>Associated Ballot:</b>	2020-03 Supply Chain Low Impact Revisions CIP-003-X AB 2 ST

There were 75 sets of responses, including comments from approximately 167 different people from approximately 114 companies representing the 10 Industry Segments as shown in the table on the following pages.

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

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Vice President of Engineering and Standards [Howard Gugel](#) (via email) or at (404) 446-9693.

## Questions

1. Do you agree the updated 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? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.
2. The standard drafting team (SDT) believes that remote access is a widely used and understood term. The team has added clarifying language to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.
3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.
4. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.
5. Do the examples in Attachment 2 Section 6 support your understanding of what is required in Attachment 1 Section 6? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.
6. 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.
7. The SDT is proposing an 18-month implementation plan for Attachment 1, Section 6.1 and 6.2. The proposed implementation time frame for Attachment 1, Section 6.3 is 24-months. Would these proposed timeframes give enough time to put into place process,

## Questions

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.

8. Provide any additional comments on the standard and technical rationale document for the standard drafting team to consider, if desired.

**The Industry Segments are:**

- 1 — Transmission Owners
- 2 — RTOs, ISOs
- 3 — Load-serving Entities
- 4 — Transmission-dependent Utilities
- 5 — Electric Generators
- 6 — Electricity Brokers, Aggregators, and Marketers
- 7 — Large Electricity End Users
- 8 — Small Electricity End Users
- 9 — Federal, State, Provincial Regulatory or other Government Entities
- 10 — Regional Reliability Organizations, Regional Entities

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
Santee Cooper	Chris Wagner	1		Santee Cooper	Jennifer Richards	Santee Cooper	1,3,5,6	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					LaChelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
					Paul Camilletti	Santee Cooper	1,3,5,6	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Susan Sosbe	Wabash Valley Power Association	3	RF
					Jennifer Bray	Arizona Electric Power	1	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Cooperative, Inc.		
					Kylee Kropp	Sunflower Electric Power Corporation	1	MRO
					Nick Fogleman	Prairie Power, Inc.	1	SERC
					Ryan Strom	Buckeye Power, Inc.	5	RF
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
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	3,5	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Fred Meyer	Algonquin Power Co.	3	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					George Brown	Acciona Energy North America	5	MRO
					Jaimin Patel	Saskatchewan Power Corporation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
LaKenya VanNorman	LaKenya VanNorman		SERC	Florida Municipal Power Agency (FMPA)	Chris Gowder	Florida Municipal Power Agency	5	SERC
					Dan O'Hagan	Florida Municipal Power Agency	4	SERC
					Carl Turner	Florida Municipal Power Agency	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Richard Montgomery	Florida Municipal Power Agency	6	SERC
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
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Power Company		
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State	7	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Reliability Council		
					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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					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	NYS PS	6	NPCC
					ALAN ADAMSON	New York State	10	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Reliability Council		
					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-Quebec 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	6	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Resources, Inc.		
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Portland General Electric Co.	Ryan Olson	5		PGE Group 2	Brooke Jockin	Portland General Electric Co.	1	WECC
					Dan Zollner	Portland General Electric Co.	3	WECC
					Daniel Mason	Portland General Electric Co.	6	WECC
					Ryan Olson	Portland General Electric Co.	5	WECC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion	5	NA - Not Applicable

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Resources, Inc.		
					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 Entity Monitoring	Steve Rueckert	WECC	10	WECC
					Phil O'Donnell	WECC	10	WECC
Lower Colorado River Authority	Teresa Krabe	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

**1. Do you agree the updated 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](#)? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.**

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

**Answer**

No

**Document Name**

**Comment**

Reclamation recommends the SDT align the CIP-003 Attachment 1 Section 6 language with CIP-005-6 R2 and use NERC-defined terms where possible. The content of Section 6 should be included within Attachment 1 Section 3 and not made into a new section. Reclamation recommends adding “if technically feasible” to Section 6.2 to account for legacy systems that are not capable of detecting known or suspected malicious communications for both inbound and outbound communications.

Reclamation recommends the following changes to Section 6:

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. Reclamation recommends using the same language as in the Technical Rationale, which refers more specifically to “when sessions are initiated.”

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT considered your recommendations and concerns to better clarify the standard language.

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

**Answer**

No

**Document Name**

**Comment**

As with the previous draft, Section 6.3 still creates a higher bar for some assets containing low impact BCS than for most medium impact BCS. Section 6.3 would require detection of malicious inbound and outbound communications for low impact BCS with vendor or remote connectivity. In the current version and next effective version of CIP-005, Part 1.5 requires detection of malicious inbound and outbound communications only for medium impact BCS at **Control Centers**.

The Technical Rationale points out that Mediums already have other requirements (“use of intermediate systems and multi-factor authentication”) which can be used to PROTECT against malicious communication; however, none of those requirements specifically

require that entities DETECT malicious communication at Mediums. Until this gap is fixed, entities will be expected to detect malicious communications at certain of their Low assets but none of their Medium assets outside of a control center.

In addition, BPA is concerned that by not properly limiting the scope statement for Section 6 to sites with vendor remote access, we may have to prove a negative.

BPA recommends the following *revision*:

Section 6. Electronic Vendor Remote Access Security Controls: For assets containing low impact BES Cyber System(s) **with vendor remote access** identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor remote access. These processes shall include...

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The drafting team has reviewed your recommendations to improve the scope, and your concerns regarding the possibility of having to prove a negative to an enforcement entity. The SDT also recognizes your concerns that the detection of malicious communications is not required for Medium impact system, and has made some clarifying changes.

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

**Answer**

No

**Document Name**

**Comment**

The introduction of “detecting known or suspected malicious communications” for low impact BES Cyber Systems would be more stringent as compared to CIP-005 R1.5 since Medium Impact BES Cyber Systems are not applicable in the current version of the standards without adding any additional reliability benefits.

Likes 0

Dislikes 0

<b>Response</b>	
Thank you for your comment. The drafting team recognizes your concerns that the detection of malicious communications is not required for Medium impact system and addressed this in the Technical Rationale (TR).	
<b>Devon Tremont - Taunton Municipal Lighting Plant - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The drafting team addressed these concerns within the TR.	
<b>Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
See EEl comment.	
Likes	0
Dislikes	0
<b>Response</b>	

Thank you for your comment. See our response to EEI.	
<b>Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
FirstEnergy feels Attachment 1 Section 6.3 is not clear in its intention of the standard and obligation of industry. We feel Attachment 1 Section 6.3 needs to be drafted to be as clear as 6.1 and 6.2	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The drafting team has further clarified the intent of Attachment 1 Section 6.3. Please see additional information in the TR.	
<b>Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
PNM supports the EEI inclusion of the word “active” in 6.1 and 6.2. However, with the inclusion of the word “active”, the current proposed language in 6.1 and 6.2 which reads, “where such access has been established under Section 3” may be redundant.	
PNM supports EEI comments regarding 6.3 to more specifically narrow the scope of detecting known or suspected malicious communications for both inbound and outbound “electronic vendor remote access, where such access has been established under section 3.”	
Likes	0

Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>patricia ireland - DTE Energy - 4</b>	
Answer	No
Document Name	
<b>Comment</b>	
Referto NAGF comment	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to NAGF.	
<b>Carl Pineault - Hydro-Qu?bec Production - 1,5</b>	
Answer	No
Document Name	
<b>Comment</b>	
Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes	0
Dislikes	0
<b>Response</b>	

Thank you for your comment. See our responses to each of your individual comments.	
<b>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</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEl) for questions #1.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEl.	
<b>Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
BC Hydro appreciates the opportunity to reeview and provides the following comments.	
BC Hydro's assessment is that 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 follow s:	
<ul style="list-style-type: none"> <li>• The language used in CIP-003-X attachment 1 Section 6.3 is referring to 'known or suspected malicious communications'. BC Hydro recommends adding more clarity and provide examples of use cases and applicability. Specifically, context and usage of the term 'malicious communication' needs more clarity and BC Hydro requests to provide the context and usage with pertinent examples and use case scenarios to improve understanding and to better scope the requirements.</li> <li>• Similarly, BC Hydro proposes defining and adding the term 'Electronic Vendor Remote Access' to NERC Glossary of Terms</li> </ul>	

- Bc Hydro also suggests that who and what is to be considered a 'Vendor' needs to be defined in the Glossary of Terms for clarity.

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 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote access; 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 6.3 completely.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The team has added clarifying information in the TR.

**Gerry Adamski - Cogentrix Energy Power Management, LLC - 5**

Answer

No

Document Name

**Comment**

For this question we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT added clarifying changes to both the language and the TR.

**Mike O'Neil - NextEra Energy - Florida Power and Light Co. - 1**

Answer

No

Document Name

## Comment

NextEra Energy respectfully submits the following language changes to Attachment 1 and Attachment 2 replacing “electronic vendor remote access” with “Vendor Electronic Remote Access” for consistency and clarification.

### Consider the following language:

#### x Attachment 1

**Section 6. Vendor Electronic Remote Access Security Controls:** 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 electronic remote access**. These processes shall include:

- 6.1** One or more method(s) for determining **vendor electronic remote access** where such access has been established under Section 3;
- 6.2** One or more method(s) for disabling **vendor electronic remote access** where such access has been established under Section 3; and
- 6.3** One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications **supporting vendor electronic remote access**.

#### CIP-003-x Attachment 2

**Section 6. Vendor Electronic Remote Access Security Controls:** Examples of evidence showing the implementation of the process for Section 6 to mitigate risks associated with **vendor electronic remote access** may include, but are not limited to:

1. For Section 6.1, documentation showing **method(s) for determining vendor electronic remote access where such access has been established under Section 3 that may including the following:**
  - steps to preauthorize access;
  - alerts generated by vendor log on;
  - session monitoring;

- Security Information Management logging alerts;
- time-of-need session initiation;
- session recording;
- system logs; or
- other operational, procedural, or technical controls.

2. For Section 6.2, documentation showing **method(s) for disabling vendor electronic remote access where such access has been established under Section 3 that may including the following:**

- disabling **vendor electronic remote access** user or system accounts;
- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active **vendor electronic remote access**;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain active **vendor electronic remote access**;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable active **vendor electronic remote access**; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of **method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor electronic access communications that may including the following:**

- Firewall policies;

- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- Virtual Private Network (VPN) hosts;
- manual log reviews; or
- other operational, procedural, or technical controls.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The drafting team has addressed these concerns in the current draft.

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

**Answer**

No

**Document Name**

**Comment**

Anything prompting action at the low impact level must be very succinct otherwise risk overwhelming already taxed resources devoted to cyber security. More detail must be developed to limit the scope of communications that will be covered.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is carefully balancing your concerns with the need to address identified cyber risks to the Bulk Electric System.

**Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance**

**Answer**

No

<b>Document Name</b>	
<b>Comment</b>	
LCRA believes the proposed language is improved upon since the last posting; however, LCRA believes it would be more clear and consistent to have the language in Attachment 1 Section 6 more closely resemble the language as written in the NERC Board resolution and the CIP-005 Standard.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The drafting team continues to try and improve the language using CIP-005 language as a reference point, however not all entities agree that CIP-005 language usage is more clear.	
<b>Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<i>The NAGF previously recommended that the SDT align the language to include the word “active”, which is utilized in both the Board Resolution and CIP-005 R2.4. The NAGF is concerned that using the word “electronic” may cause a differing definition and expectation to be developed over time compared to the objective of the language in the Board Resolution. Does the SDT view “active” and “electronic” as synonymous terms? If the SDT does not see “active” and “electronic” remote vendor access as synonymous further definition of “electronic” is required.</i>	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your comments. The drafting team does not see the terms “active” and “electronic” as synonymous. There were many comments asking for clarity of the term “active” in the last posting, some feeling that it was not limited to remote electronic communications. The SDT made clarifying changes to both the standard language and the TR.

**James Baldwin - Lower Colorado River Authority - 1**

**Answer** No

**Document Name**

**Comment**

LCRA believes the proposed language is improved upon since the last posting; however, LCRA believes it would be more clear and consistent to have the language in Attachement 1 Section 6 more closely resemble the language as written in the NERC Board re resolution and the CIP-005 Standard.

Likes 0

Dislikes 0

**Response**

Thank you for your comments. The drafting team does not see the terms “active” and “electronic” as synonymous. There were many comments asking for clarity of the term “active” in the last posting, some feeling that it was not limited to remote electronic communications. The SDT made clarifying changes to both the standard language and the TR.

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

**Answer** No

**Document Name**

**Comment**

EI recognizes that the proposed changes under this project are intended to align with the NERC Board resolution, however, EEI is concerned that the proposed Draft 2 language in Attachment 1, Section 6 goes beyond the intent of the Board resolution by being overly broad. In addition, the proposed language in Section 6 is not risk-based and could be understood to mean all low impact BES Cyber System communications are included. As a result, entities would be faced with difficult choices that include how to safely allocate scarce

resources (i.e., limited budgets and qualified SMEs) to meet existing CIP-003 requirements while also covering the unfettered expansion of low impact BES Cyber System communications. To address this concern, we ask that the SDT employ a risk-based approach that allows entities to develop processes that focus their resources on those systems that represent known risks.

In addition to the above concern, EEI supports the proposed language in Section 6, subparts 6.1 and 6.2 but suggests some minor edits as indicated in the bold text below. In particular the proposed language for subpart 6.3 is not sufficiently aligned with communications as established under Section 3. The introduction of the new undefined term “vendor communications” needs additional explanation or clarification because it is treated separately and not aligned with Section 3. For these reasons, we recommend adding the text in bold to define the scope more clearly.

**Section 6:** Electronic Vendor Remote Access Security Controls: 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 vendor remote access. These process shall include:

6.1: One or more method(s) for determining **when active** electronic vendor remote access **has been initiated**; where such access has been established under Section 3;

6.2: One or more method(s) for disabling **active** electronic vendor remote access **when necessary**; where such access has been established under Section 3; and

6.3: One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound **electronic vendor remote access, where such access has been established under Section 3.**

Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The drafting team has addressed these concerns in the current draft.	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee</b>	
<b>Answer</b>	No
<b>Document Name</b>	

**Comment**

Based on the comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT believes we have met the requirements of the current SAR.

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

**Answer**

No

**Document Name**

**Comment**

The language used in of the NERC Board resolution states the CIP-003 is “to include policies for low impact BES Cyber Sytems...”. We agree with the SDT’s interpretation that 3 controls listed in the resolution should be addressed not only in the CIP -003 R1.2, policies but in the plans required in CIP-003 R2 and Attachment 1. While the R2 additions are an expansion beyond the NERC Board resolution, they are required to meet the intent of the resolution.

Because CIP-003 Attachment 1 is written to apply at the “assets containing low impact BES Cyber Systems” and not to just the “BES Cyber Systems”, the 3 controls listed in the NERC Board resolution could be required to be applied to more than low impact BCS. This expansion in scope beyond low impact BCS is not required by the NERC Board resolution. The expansion could include additional controls being required for medium and high impact Cyber Assets beyond what are included in as “Applicable Systems” in CIP-005 R1.5 and R3. Regarding the control concerning malicious communication, we feel that this should be limited to only low impact BCS at Control Centers to align with CIP-005 R1.5.

An interpretation of what the SDT has proposed could require the detection of malicious voice communication, text messages, or emails from anyone to anyone that is at an asset containing low impact BES Cyber Systems.

The NERC Board resolution includes the implementation of controls to “disable active vendor remote access.” CIP-005 R2.5 addresses disabling active vendor remote access and R3.2 addresses terminating vendor initiated remote connections. The actions listed in Attachment 2 and the language used in the Technical Rational for Attachment 1 Section 6 Part 6.2 combine disabling and terminating as part of the required control. The SDT should limit the scope to disabling active vendor remote access.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. The SDT updated language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6 to better define the communication s scope. The SDT updated the TR to use the term “disable” instead of “terminate” to be consistent with the draft standard language.

**Daniel Gacek - Exelon - 1**

**Answer**

No

**Document Name**

**Comment**

Exelon believe registered entities could accomplish this, however it would be difficult to tell what the malicious intent really is. We do understand, however IDS can help with the inspection of packets. But without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term “vendor communications” needs explanation.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. Additionally, the term “vendor communications” has been removed from the draft standard.

**Kinte Whitehead - Exelon - 3**

**Answer** No

**Document Name**

**Comment**

Exelon believe registered entities could accomplish this, however it would be difficult to tell what the malicious intent really is. We do understand, however IDS can help with the inspection of packets. But without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term “vendor communications” needs explanation.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. Additionally, the term “vendor communications” has been removed from the draft standard.

**Kimberly Turco - Constellation - 6**

**Answer** No

**Document Name**

**Comment**

Constellation has elected to align with Exelon in response to this question.

Entities could accomplish this, however it could be difficult to tell what malicious intent really is. We do understand IDS can help with the inspection of packets. Without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term “vendor communications” needs explanation.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. Additionally, the term “vendor communications” has been removed from the draft standard.

**Alison Mackellar - Constellation - 5**

**Answer**

No

**Document Name**

**Comment**

Constellation has elected to align with Exelon in response to this question.

Entities could accomplish this, however it could be difficult to tell what malicious intent really is. We do understand IDS can help with the inspection of packets. Without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term “vendor communications” needs explanation.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. Additionally, the term “vendor communications” has been removed from the draft standard.

**Jamie Monette - Allele - Minnesota Power, Inc. - 1**

**Answer** No

**Document Name**

**Comment**

Minnesota Power is in agreement with Edison Electrical Institute’s (EEI) comments and believes the drafted language more adequately addresses the purpose/goal as stated in the SAR and Technical Rationale

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to EEI.

**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, Group Name Florida Municipal Power Agency (FMPA)**

**Answer** No

**Document Name**

**Comment**

FMPA supports comments from Utility Services, Inc.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to Utility Services, Inc.	
<b>Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Portland General Electric Company (PGE) supports the survey response provided by EEI.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to EEI comments.	
<b>Russell Noble - Cowlitz County PUD - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to Utility Services, Inc.	
<b>Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh</b>	

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
NST notes that the NERC BoT's resolution, as written, does not explicitly limit the application of a malicious code detection requirement to remote connections to or from vendors.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT had several conversations about this topic with NERC compliance and legal staff. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access.	
<b>Daniel Mason - Portland General Electric Co. - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Deanna Carlson - Cowlitz County PUD - 5</b>	
<b>Answer</b>	No

<b>Document Name</b>	
<b>Comment</b>	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to Utility Services, Inc.	
<b>Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
While we agree with the updated language as a whole, we support EEI's proposed modification to Attachment 1 Section 6, as it adds clarity.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

Comment	
No comment	
Likes 0	
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 0	
Dislikes 0	
Response	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	

While the proposed language addresses the risks outlined by the NERC Board resolution, adding the word “vendor”, not a NERC defined term, to the requirement from the previously posted: “One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications” doesn’t materially change this requirement is more stringent than those required by CIP-005 R1.5 for medium impact BES Cyber Systems NOT at Control Centers. Further reducing the scope of the requirement to only vendor communications, we don’t feel reduces risks to an acceptable level for NERC or FERC. If entities are going to be required to detect malicious communications, it should be all or nothing. Additionally, vendor is not a NERC defined term, so having to prove each monitored communication path is or isn’t for a vendor would be overly burdensome.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT had several conversations with NERC compliance and legal staff about this topic. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access. Also see the draft TR for a discussion on vendor.

**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**

Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

**Answer** Yes

**Document Name**

**Comment**

AEPCO is signing on to ACES comments below:

ACES Comments: While the proposed language addresses the risks outlined by the NERC Board resolution, adding the word “vendor”, not a NERC defined term, to the requirement from the previously posted: “One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications” doesn’t materially change this requirement is more stringent than those required by CIP-005 R1.5 for medium impact BES Cyber Systems NOT at Control Centers. Further reducing the scope of the requirement to only vendor communications, we don’t feel reduces risks to an acceptable level for NERC or FERC. If entities are going to be required to detect malicious communications, it should be all or nothing. Additionally, vendor is not a NERC defined term, so having to prove each monitored communication path is or isn’t for a vendor would be overly burdensome.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT had several conversations with NERC compliance and legal staff about this topic. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access. Also see the draft TR for a discussion on vendor.

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

**Answer** Yes

**Document Name**

<b>Comment</b>	
The MRO NERC Standards Review Forum (NSRF) agrees proposed language addresses the risk.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
<b>George Brown - Acciona Energy North America - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this questi on.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	

We agree because this gives the ability to disconnect, we ask the drafting team to include examples of evidence for this requirement (logs?).	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT provided examples of evidence for Section 6 in Attachment 2.	
<b>Mike Magruder - Avista - Avista Corporation - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
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
<b>Response</b>	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums has been discussed in the TR.	
<b>Brian Lindsey - Entergy - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	

No Comment	
Likes	0
Dislikes	0
<b>Response</b>	
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	
<b>Comment</b>	
<p>While the proposed language addresses the risks outlined by the NERC Board resolution, adding the word “vendor”, not a NERC defined term, to the requirement from the previously posted: “One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications” doesn’t materially change this requirement is more stringent than those required by CIP-005 R1.5 for medium impact BES Cyber Systems NOT at Control Centers. Further reducing the scope of the requirement to only vendor communications, we don’t feel reduces risks to an acceptable level for NERC or FERC. If entities are going to be required to detect malicious communications, it should be all or nothing. Additionally, vendor is not a NERC defined term, so having to prove each monitored communication path is or isn’t for a vendor would be overly burdensome.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<p>Thank you for your comment. The SDT had several conversations with NERC compliance and legal staff about this topic. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access. Also see the draft TR for a discussion on vendor.</p>	

**Benjamin Winslett - Georgia System Operations Corporation - 4**

<b>Answer</b>	Yes
<b>Document Name</b>	<a href="#">2020-03_Supply_Chain_Lows_Unofficial_Comment_Form.docx</a>

**Comment**

While GSOC agrees that the proposed language addresses the risks identified by the NERC Board Resolution, it is concerned that the absence of the term “active” broadens this requirement beyond the obligations set forth to manage vendor access for medium and high impact BES cyber assets. In particular, the language of the similar requirements for vendor access management in CIP-005-7, R2.4 and R2.5 focuses the requirements on determining and disabling “active vendor remote access sessions.” The language proposed in Attachment 1, Sections 6.1 and 6.2, however, could be interpreted to apply to any authorized vendor remote access – regardless of whether or not the vendor has initiated or is in an active remote access session.

Such a requirement would result in low impact BES cyber assets being subject to more stringent security controls than high or medium impact BES cyber assets and appears to conflict with the Technical Rationale for these sections as provided on page 5 of the proposed Technical Rationale document. To ensure that the security controls applied to low impact BES cyber assets are commensurate with risk and not more stringent than those applied to high and medium impact BES cyber assets, GSOC recommends that the SDT mirror the language provided in CIP-005-7, R2.4 and R2.5 to the extent possible. For example, revisions could be made as follows:

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 vendor remote access. These processes shall include:

6.1 One or more method(s) for determining active electronic vendor remote access sessions where such access has been established under Section 3;

6.2 One or more method(s) for disabling active electronic vendor remote access where such access has been established under Section 3

Likes	0
Dislikes	0

**Response**

Thank you for your comment. The SDT discussed the addition of the term “active” in section 6. The team decided that stating “as established under Section 3.1” meets the objective of the Board resolution. The SDT is attempting to make the language risk-based and

believes it is currently drafted to allow entities to draft their program in a way that meets their unique set up in regards to vendor remote access.

Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.

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

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

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

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC**

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Martin Sidor - NRG - NRG Energy, Inc. - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes	0
Dislikes	0
<b>Response</b>	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name</b> Tennessee Valley Authority	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Chris Wagner - Santee Cooper - 1, Group Name</b> Santee Cooper	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Mike Marshall - IDACORP - Idaho Power Company - 1</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Donald Lock - Talen Generation, LLC - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>JT Kuehne - AEP - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsey Mannion - ReliabilityFirst - 10</b>	
<b>Answer</b>	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Fong 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; - Tim Kelley	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Israel Perez - Salt River Project - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
<b>Larry Heckert - Alliant Energy Corporation Services, Inc. - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Donna Wood - Tri-State G and T Association, Inc. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<p>Texas Re appreciates the SDT and NERC legal looking into the issue of whether or not Part 1 of the NERC resolution has been satisfied. Texas RE suggests the SAR and the report do provide flexibility for the SDT to consider language for detecting known or suspected malicious communications for all inbound and outbound communications, and not be limited to vendor inbound and outb ound communications. Texas RE continues to recommend 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 notes this approach is consistent with FERC’s January 20, 2022 Notice of Proposed Rulemaking (NOPR) regarding internal network security monitoring.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<p>Thank you for your comment. The SDT had several conversations with NERC compliance and legal staff about this topic. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Also see the draft TR for a discussion on vendor.</p>	
<b>Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	

Xcel Energy agrees that Attachment 1 Section 6 addresses the risk malicious communication posed by vendors accessing low impact BES cyber systems from remote locations. However, there is a lack of clarity of which types of cyber assets are in scope for sub part 6.3. Xcel Energy suggests that language of "as established in section 3" be added to section 6.3 as it is in sections 6.1 and 6.2.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6.

**John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway**

**Answer**

**Document Name**

**Comment**

No comment.

Likes 0

Dislikes 0

**Response**

<b>2. The standard drafting team (SDT) believes that remote access is a widely used and understood term. The team has added clarifying language to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification .</b>	
<b>Deanna Carlson - Cowlitz County PUD - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you, please see our response to Utility Services, Inc.	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Header 6.1 and 6.2 - Add the word “active” in the requirement and move “electronic” adjective. One or more method(s) for determining <i>active vendor electronic</i> remote access where such access has been established in Section 3.	
Likes	0
Dislikes	0

Response	
Thank you for your comments. The SDT made clarifying changes to the current draft.	
<b>Daniel Mason - Portland General Electric Co. - 6</b>	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes	0
Dislikes	0
Response	
Thank you, please see our response to EEI.	
<b>Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh</b>	
Answer	No
Document Name	
Comment	
NST suggests dropping "electronic" from the phrase, "electronic vendor remote access." The only kind of remote access to electronic devices (including Cyber Assets) that presently exists is electronic. In addition, NST believes the remote access terms the SDT has used in CIP-003 Sections 6.1, 6.2 and elsewhere should be consistent with the language in CIP-005, which addresses "vendor remote access," not "electronic vendor remote access." Consistent use of terms enables Responsible Entities with assets other than low impact to develop and apply controls across assets of differing impact levels.	
Likes	0
Dislikes	0

**Response**

Thank you for your comment. We understand the premise you are stipulating, however we have had comments as to whether remote access might also include the insertion of a thumb drive and dial up access into a system. The SDT made clarifying changes to both the standard language and the TR. The SDT added the word “electronic” to ensure that dial up connectivity or other non-electronic access, which could be considered remote by some, was not included in the requirements of this standard. Additionally, we have received comments regarding the use of the same terms as those in CIP-005, because it is believed the definition of the term used in CIP-005 is broader than the intent of the SAR and NERC in requiring the development of this standard.

**Russell Noble - Cowlitz County PUD - 3**

**Answer** No

**Document Name**

**Comment**

Cowlitz PUD supports the comments submitted by Utility Services Inc.

Likes 0

Dislikes 0

**Response**

Thank you, please see our response to Utility Services, Inc.

**Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2**

**Answer** No

**Document Name**

**Comment**

PGE supports the survey response provided by EEI.

Likes 0

Dislikes	0
<b>Response</b>	
Thank you, please see our response to EEI.	
<b>Jamie Monette - Allete - Minnesota Power, Inc. - 1</b>	
Answer	No
Document Name	
<b>Comment</b>	
Minnesota Power is in agreement with Edison Electric Institute’s (EEI) comments. Draft 1 of Attachment 1 Section 6 included the clarifying language “(including interactive and system-to-system access)” which was removed from Draft 2, making it unclear what forms of access are in scope. Additionally, the term “vendor” is an undefined term and should be clarified in the NERC Glossary of Terms.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you, please see our response to EEI.	
<b>Alison Mackellar - Constellation - 5</b>	
Answer	No
Document Name	
<b>Comment</b>	
Constellation has elected to align with Exelon in response to this question.	
Exelon doesn’t agree that it’s necessarily clear so can’t agree that its widely understood. The term ‘Remote’ can mean different things...a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card... or is it up to the Registered Entity to define it?	

Likes	0
Dislikes	0
<b>Response</b>	
Thank you, please see our response to Exelon.	
<b>Kimberly Turco - Constellation - 6</b>	
Answer	No
Document Name	
<b>Comment</b>	
<p>Constellation has elected to align with Exelon in response to this question.</p> <p>Exelon doesn't agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things...a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card... or is it up to the Registered Entity to define it?</p>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you, please see our response to Exelon.	
<b>Kinte Whitehead - Exelon - 3</b>	
Answer	No
Document Name	
<b>Comment</b>	

<p>Exelon does not agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things...a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card... or is it up to the Registered Entity to define it?</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<p>Thank you for your comment. The drafting team has provided more information on "remote" in the TR.</p>	
<b>Daniel Gacek - Exelon - 1</b>	
Answer	No
Document Name	
<b>Comment</b>	
<p>Exelon does not agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things...a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card... or is it up to the Registered Entity to define it?</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<p>Thank you for your comment. The drafting team has provided more information on "remote" in the TR.</p>	
<b>Brian Evans-Mongeon - Utility Services, Inc. - 4</b>	
Answer	No
Document Name	
<b>Comment</b>	

The SDT has used the word “electronic vendor remote access” and not the term “active vendor remote access” that is used in CIP-005-7 and in the NERC Board resolution. It is unclear why this inconsistency is needed or what the difference is between the two terms.

Furthermore when reviewing the Technical Rationale behind these proposed modifications, a footnote which had previously referenced guidance on the term “vendor” and how it may be used in the current version of CIP-013 and the future versions of CIP-005, CIP-010, and CIP-013, had been removed making for more confusion on what a vendor may be in this scope. Can the SDT please provide the reasoning for removing the footnote/reference from the Technical Rationale?

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT made these changes based on comments from a previous ballot and comment period.

**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 using the CIP terms “interactive remote access” and “system-to-system access” instead of introducing a new term “Electronic vendor remote access.” Also, CIP-005 uses “vendor remote access.” Remote access implies “electronic” so “electronic” does not need inclusion in the term.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT previously received comments regarding the use of the terms included in CIP-005, because they are defined in a manner which may broaden the scope of the language drafted for CIP-003. The SDT made clarifying changes to the standard as well as the TR.

<b>Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
While the term “remote access” is generally understood, it is unclear what it means in the context of this Reliability Standard. Specifically, it is unclear whether the SDT meant this to mean user remote access, machine remote access or both. For this reason, we ask that the SDT provide clearer direction within the Technical Rationale.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The drafting team has provided more information on “remote” in the TR.	
<b>Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
More work should be undertaken to clearly define the terms remote access and the scenarios.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The drafting team has provided more information on “remote” in the TR.	
<b>Brian Lindsey - Entergy - 1</b>	
<b>Answer</b>	No

<b>Document Name</b>	
<b>Comment</b>	
Generally “interactive” remote access is also used. Interactive means not only read only or view only access. This should be a part of the standard as if I am only viewing or retrieving read only data there is no ability for the remote connection to make changes or perform actions.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The drafting team has provided more information on “remote” in the TR.	
<b>Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Please see NEE’s response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to NEE, question 1.	
<b>Gerry Adamski - Cogentrix Energy Power Management, LLC - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	

**Comment**

Recommend using the CIP terms of “interactive remote access” and “system-to-system access” instead of introducing a new term “Electronic vendor remote access.” Also, CIP-005 uses “vendor remote access.” Remote access implies “electronic” so “electronic” does not need inclusion in the term.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The term “interactive remote access” was removed due to comments received during a previous posting. The SDT added the word “electronic” to ensure that dial up connectivity was not included in the requirements of this standard.

**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, ' Electronic Vendor Remote Access' needs additional clarity to ensure proper understanding of applicability as well as the use of term 'Vendor' e.g., whether consultant using same infrastructure is considered vendor?

Likes 0

Dislikes 0

**Response**

Thank you for your comments. The SDT added the word “electronic” to ensure that dial up connectivity was not included in the requirements of this standard. Also see the draft TR for a discussion on vendor.

**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**

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #2.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Carl Pineault - Hydro-Qu?bec Production - 1,5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Recommend using the CIP terms of “interactive remote access” and “system-to-system access” instead of introducing a new term “Electronic vendor remote access.” Also, CIP-005 uses “vendor remote access.” Remote access implies “electronic” so “electronic” does not need inclusion in the term.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comments. The decision to remove the terms “interactive remote access” and “system to system remote access” was based on comments to a previous posting of this standard. The SDT added the word “electronic” to ensure that dial-up connectivity and/or use of removable media was not included in the requirements of this standard.	
<b>Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1</b>	

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
PNM supports EEI comments regarding the needed clarity around “remote access” referring to user remote access, machine remote access, or both.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
FirstEnergy agrees with EEI’s comments: “While the term “remote access” is generally understood, it is unclear what it means in the context of this Reliability Standard. Specifically, it is unclear whether the SDT meant this to mean user remote access, machine remote access or both. For this reason, we ask that the SDT provide clearer direction within the Technical Rationale.”	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker</b>	

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
See EEI comment.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Israel Perez - Salt River Project - 1,3,5,6 - WECC</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
SRP would like to see “Electronic Vendor Remote Access” as a clearly defined term. For example, is web-conferencing considered electronic vendor remote access?	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your response. The drafting team has provided more information on “remote” in the TR.	
<b>Devon Tremont - Taunton Municipal Lighting Plant - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	

<b>Comment</b>	
Recommend using the CIP terms of “interactive remote access” and “system-to-system access” instead of introducing a new term “Electronic vendor remote access.”	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT removed the terms “interactive remote access” and “system to system remote access” based on feedback from a previous comment period for this standard over concerns that those terms expanded the scope of the SAR for this update.	
<b>Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Southern Indiana Gas and Electric (SIGE) does not believe that this language is clear or widely used. The most widely used description of remote access is interactive remote access. If the SDT intends to include system-to-system access then that should be made clear. Remote access should be clearly defined as interactive access and system-to-system remote access. SIGE proposes re-installing the wording from Draft 1 Attachment 1 Section 6 to give additional detail to remote access, “(including interactive and system-to-system access) to low impact BES Cyber Systems.”	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT removed the terms “interactive remote access” and “system to system remote access” based on feedback from a previous comment period for this standard over concerns that those terms expanded the scope of the SAR.	

<b>Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Remote access should be clearly defined as including interactive and system-to-system remote access. CenterPoint Energy Houston Electric (CEHE) proposes re-instating the wording from Draft 1 Attachment 1 Section 6 to give additional detail to remote access, “(including interactive and system-to-system access) to low impact BES Cyber Systems.”	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT removed the terms “interactive remote access” and “system to system remote access” based on feedback from a previous comment period for this standard over concerns that those terms expanded the scope of the SAR.	
<b>Martin Sidor - NRG - NRG Energy, Inc. - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
If “remote access” is going to be brought into scope for low impact sites and the intent is for it to be limited strictly to remote access conducted by vendors, then the term needs to be in alignment with the “Interactive Remote Access” definition. The manner in which Section 6 is currently written seems to imply that system-to-system communications will be included.	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your comment. The SDT received contrary responses with the belief that using the term “Interactive Remote Access” expands the scope of the SAR because of its formal definition in the [NERC Glossary of Terms](#).

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

**Answer** No

**Document Name**

**Comment**

Reclamation recommends adding “Vendor” to the NERC Glossary of Terms and proposes the following definition:

Vendor - Persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts to supply equipment for BES Cyber Systems and related services. Vendor does not include other NERC-registered entities that provide reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). Vendor 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**

Thank you for your comment. The SDT addressed the term “vendor” in the TR.

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

**Answer** No

**Document Name**

**Comment**

If “remote access” is going to be brought into scope for low impact sites and the intent is for it to be limited strictly to remote access conducted by vendors, then the term needs to be in alignment with the “Interactive Remote Access” definition. The manner in which Section 6 is currently written seems to imply that system-to-system communications will be included.

Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT received contrary responses with the belief that using the term “Interactive Remote Access” expands the scope of the SAR because of its formal definition in the <a href="#">NERC Glossary of Terms</a> .	
<b>Benjamin Winslett - Georgia System Operations Corporation - 4</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
GSOC agrees that remote access is a widely used and understood term and would suggest that the language used in Attachment 1 more closely mirror the language utilized in CIP-005-7 to reduce the potential for additional confusion, ambiguity, and subjective interpretation. Please see comments provided in response to question 1 above.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. See our response to question 1.	
<b>Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
<i>The NAGF has no comments.</i>	
Likes	0

Dislikes	0
<b>Response</b>	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
<b>Comment</b>	
The language is more clear, but does not really limit the effort to implement the control.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
<b>Comment</b>	
Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this questi on.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you, please see our response to MRO NSRF.	

<b>Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
The MRO NSRF believes that the language is properly scoped.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Xcel Energy believes that the term "remote access" is commonly used to address electronic access originating from locations outside of protections established in an entities PSP and ESP.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Scott Kinney - Avista - Avista Corporation - 3</b>	
<b>Answer</b>	Yes

<b>Document Name</b>	
<b>Comment</b>	
The language is more clear, but does not really limit the effort to implement the control.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Glen Farmer - Avista - Avista Corporation - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
The language is more clear, but does not really limit the effort to implement the control.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

We believe that the language is clear.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>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, Group Name Florida Municipal Power Agency (FMPA)</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
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	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Donna Wood - Tri-State G and T Association, Inc. - 1</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Larry Heckert - Alliant Energy Corporation Services, Inc. - 4</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>patricia ireland - DTE Energy - 4</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Susan Sosbe - Wabash Valley Power Association - 3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Fong 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; - Tim Kelley</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jesus Sammy Alcaraz - Imperial Irrigation District - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Michelle Amarantos - APS - Arizona Public Service Co. - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsey Mannion - ReliabilityFirst - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>JT Kuehne - AEP - 6</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Donald Lock - Talen Generation, LLC - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Mike Marshall - IDACORP - Idaho Power Company - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
No comment.	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor’s access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.</b>	
<b>Patricia Lynch - NRG - NRG Energy, Inc. - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Comments: Remote access, as widely understood today with regards to the CIP standards, involves interactive electronic access across an Electronic Security Perimeter. Low impact sites do not have an associated requirement for an Electronic Security Perimeter, so there is no reference point for what is considered a “remote location”.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT realized that IRA across an ESP is the requirement for both High and Med, however, since neither of those definitions apply to Lows, the team included the language “as established within Attachment 1 Section 3.1”. Section 3 for Lows is the requirement to create a network boundary for access to the low impact BES Cyber Systems from Cyber Assets outside the asset containing low impact BES Cyber Systems. Since this requirement has been in place for some time, the SDT believes “remote access” is any access that crosses this boundary.	
<b>Richard Jackson - U.S. Bureau of Reclamation - 1,5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	

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
<b>Response</b>	
Thank you for your comment. The SDT included the language “as established within Attachment 1 Section 3.1”. Section 3 for Lows is the requirement to create a network boundary for access to the low impact BES Cyber Systems from Cyber Assets outside the asset containing low impact BES Cyber Systems. Since this requirement has been in place for some time, the SDT believes “remote access” is any access that crosses this boundary. If a vendor is “onsite” but starts the connection process outside this boundary, this connection should be considered remote access.	
<b>Martin Sidor - NRG - NRG Energy, Inc. - 6</b>	
Answer	No
Document Name	
<b>Comment</b>	
Remote access, as widely understood today with regards to the CIP standards, involves interactive electronic access across an Electronic Security Perimeter. Low impact sites do not have an associated requirement for an Electronic Security Perimeter, so there is no reference point for what is considered a “remote location”.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT realized that IRA across an ESP is the requirement for both High and Med, however, since neither of those definitions apply to Lows, the SDT included the language “as established within Attachment 1 Section 3.1”. Section 3 for Lows is the requirement to create a network boundary for access to the low impact BES Cyber Systems from Cyber Assets outside the asset	

containing low impact BES Cyber Systems. Since this requirement has been in place for some time, the SDT believes “remote access” is any access that crosses this boundary.

**Devon Tremont - Taunton Municipal Lighting Plant - 1**

**Answer** No

**Document Name**

**Comment**

Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed. The Cyber Assets identified as medium impact would not be applicable to Section 6.

**Carl Pineault - Hydro-Quebec Production - 1,5**

**Answer** No

**Document Name**

**Comment**

Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level.

Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.

Likes 0

Dislikes 0

Response	
<p>Thank you for your comment. The SDT believes that the changes made to add this requirement have not impacted the way that mixed environments are currently being addressed. The Cyber Assets identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.</p>	
<p><b>Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro</b></p>	
Answer	No
Document Name	
Comment	
<p>BC Hydro suggests that the use of word "Remote" will need clarification and perhaps a definition in the Glossary of Terms. For example, in the scenarios below, how will the "Remote" term be used?</p> <ol style="list-style-type: none"> <li>1. On site, but electronically remote (i.e. has to go through EAP despite being at the station).</li> <li>2. A "vendor" at the work location of Responsible Entity, also electronically remote (i.e. going through EAP).</li> <li>3. "Traditionally" remote, off site, and electronically remote (also going through EAP).</li> </ol>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The SDT included the language “as established within Attachment 1 Section 3.1”. Section 3 for Lows is the requirement to create a network boundary for access to the low impact BES Cyber Systems from Cyber Assets outside the asset containing low impact BES Cyber Systems. Since this requirement has been in place for some time, the SDT believes “remote access” is any access that crosses this boundary.</p>	
<p><b>Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1</b></p>	
Answer	No
Document Name	
Comment	

Please see NEE’s response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to question 1.	
<b>Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF</b>	
Answer	No
Document Name	
<b>Comment</b>	
<i>The NAGF membership is concerned with the “remote locations” language in this question. Remote location is not used to describe the vendor’s access in any version of the standard language. Is the SDT referencing geographic location or network topology? The standard language references inbound and outbound communications between the BES Cyber System and “Cyber Asset(s) outside the asset” (Section 3.1.i).</i>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The concept presented by the SDT is that “remote” is based on the criteria established with Attachment 1, Section 3.1.	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee</b>	
Answer	No
Document Name	

**Comment**

Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level.

Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed.

The Cyber Assets that are identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.

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

**Answer**

No

**Document Name**

**Comment**

We disagree that the intent of the NERC Board resolution is to address vendor access to low impact assets. Our understanding of the NERC Board resolution is that the controls are to apply to low impact BES Cyber Systems at assets that have low impact BES Cyber Systems. The SDT's interpretation could require the 3 controls to be applied to vendor remote access and communication to more than not just low impact BCS.

Likes 0

Dislikes 0

<b>Response</b>	
Thank you for your comment. While we agree the resolution is focused on the risk of vendor remote access to low impact BES cyber systems, the SDT believes the draft language is consistent with other sections of Attachment 1.	
<b>Daniel Gacek - Exelon - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Exelon ultimately believes this would require us to have an inventory list of the lows impact assets.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The team believes the drafted language requires no more than what is required today to meet the other sections of Attachment 1.	
<b>Kinte Whitehead - Exelon - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Exelon believe that ultimately, this would require us to have an inventory list of the lows impact assets.	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your comment. The team believes the drafted language requires no more than what is required today to meet the other sections of Attachment 1.	
<b>Kimberly Turco - Constellation - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
The new undefined term “vendor communications” needs additional explanation. Recommend adding text in bold for clarity. In sections 6.1-6.3 the SDT should consider using “active” electronic vendor remote access and in 6.3 add “...where such access has been established under section 3”	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT added language about “access being established under Section 3.1” to the parent so it applies to the subparts of Section 6.	
<b>Alison Mackellar - Constellation - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
The new undefined term “vendor communications” needs additional explanation. Recommend adding text in bold for clarity. In sections 6.1-6.3 the SDT should consider using “active” electronic vendor remote access and in 6.3 add “...where such access has been established under section 3”	
Likes 0	
Dislikes 0	

**Response**

Thank you for your comment. The SDT added language about “access being established under Section 3.1” to the parent so it applies to the subparts of Section 6.

**Russell Noble - Cowlitz County PUD - 3**

**Answer** No

**Document Name**

**Comment**

Cowlitz PUD supports the comments submitted by Utility Services Inc.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to Utility Services, Inc.

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

**Answer** No

**Document Name**

**Comment**

“Vendor communications” is a new term. It doesn’t scope this new term to communications “as established in Section 3” as the others do. “Vendor communications” is too broad of a term and wide open to many interpretations of the definition meaning.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT adjusted the language to help better clarify this term.

<b>Deanna Carlson - Cowlitz County PUD - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to Utility Services, Inc.	
<b>Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Yes, the SDT has clarified the scope.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
<b>Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

Comment	
No 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 Hirschak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy belives the scope is clear.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
<b>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</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEl) for questions #3.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to EEl.	
<b>Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
The MRO NSRF believes that the language is properly scoped.	

Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>George Brown - Acciona Energy North America - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this questi on.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to MRO NSRF.	
<b>Brian Lindsey - Entergy - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
No Comment	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
EEI agrees in part that the language in Attachment 1, Section 6 is clear but offers some suggested edits for SDT consideration. (See our response to Question 1)	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to question 1.	
<b>Jamie Monette - Allete - Minnesota Power, Inc. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Minnesota Power is in agreement with Edison Electric Institute's (EEI) comments.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Although NST agrees Section 6 applies only to vendor remote access, it is our opinion that a malicious code detection requirement should not be limited to only vendor remote connections.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The NERC Board Resolution, and the subsequent approved SAR, focused the drafting team’s work on vendor communications. It is outside the scope of the SAR to expand on that at this time.	
<b>Daniel Mason - Portland General Electric Co. - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

Comment	
PGE supports the survey response provided by EEL.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEL.	
<b>Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
<b>Response</b>	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mike Marshall - IDACORP - Idaho Power Company - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Donald Lock - Talen Generation, LLC - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>JT Kuehne - AEP - 6</b>	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsey Mannion - ReliabilityFirst - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Michelle Amarantos - APS - Arizona Public Service Co. - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Glen Farmer - Avista - Avista Corporation - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Jesus Sammy Alcaraz - Imperial Irrigation District - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Fong 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; - Tim Kelley</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Israel Perez - Salt River Project - 1,3,5,6 - WECC</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Susan Sosbe - Wabash Valley Power Association - 3</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Scott Kinney - Avista - Avista Corporation - 3</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>patricia ireland - DTE Energy - 4</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Larry Heckert - Alliant Energy Corporation Services, Inc. - 4</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Donna Wood - Tri-State G and T Association, Inc. - 1</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Gerry Adamski - Cogentrix Energy Power Management, LLC - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mike Magruder - Avista - Avista Corporation - 1</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>James Baldwin - Lower Colorado River Authority - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller</b>	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Benjamin Winslett - Georgia System Operations Corporation - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>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, Group Name Florida Municipal Power Agency (FMPA)</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Vendor remote access needs to be clear to convey remote access only	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT made updates to the draft standard to clarify.	
<b>John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
No comment.	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>4. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.</b>	
<b>Deanna Carlson - Cowlitz County PUD - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to Utility Services, Inc.	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
6.3 language needs to be clearer and have a tighter bounded scoping to avoid the widest possible interpretation at audit. You can't go to Section 3 Electronic Access Controls evidence and show you are detecting things on all identified LERC and fully prove 6.3 as it is currently written. The intent of 6.3 should be added as a requirement to Section 3.	
Likes	0
Dislikes	0

<b>Response</b>	
Thank you for your comment. The SDT made modifications to the proposed language in Section 6.3 to more closely tie it to the scope of Sections 3.1.	
<b>Daniel Mason - Portland General Electric Co. - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
PGE supports the survey response provided by EEI.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Russell Noble - Cowlitz County PUD - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to Utility Services, Inc.	

<b>Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Alison Mackellar - Constellation - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Constellation has elected to align with Exelon in response to this question.	
Exelons interpretation of the proposed standard views that this opens up access to 'any' areas that has a low.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to Exelon.	
<b>Kimberly Turco - Constellation - 6</b>	

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Constellation has elected to align with Exelon in response to this question.</p> <p>Exelons interpretation of the proposed standard views that this opens up access to ‘any’ areas that has a low.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to Exelon.	
<b>Kinte Whitehead - Exelon - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Exelons interpretation of the proposed standard views that this opens up access to ‘any’ areas that contain lows.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.	
<b>Daniel Gacek - Exelon - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	

Comment	
Exelons interpretation of the proposed standard views that this opens up access to ‘any’ areas that has a low	
Likes	0
Dislikes	0
Response	
Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.	
<b>Brian Evans-Mongeon - Utility Services, Inc. - 4</b>	
Answer	No
Document Name	
Comment	
The proposed language in Section 6.3 could be interpreted to include communication to people and all Cyber Assets at an asset that contains low impact BCS. The controls for active vendor remote access could also be required to be applied to all Cyber Assets at the asset and not just those that are part of a low impact BCS.	
We would suggest appending a statement consistent with the other two subsections of Section 6, “where such access has been established under Section 3.”	
Likes	0
Dislikes	0
Response	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3” applies to all parts of Section 6.	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee</b>	
Answer	No

<b>Document Name</b>	
<b>Comment</b>	
<p>Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level.</p> <p>Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<p>Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed. Cyber Assets identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.</p>	
<b>Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>EI disagrees that the language in Attachment 1, Section 6 clearly limits the scope to low impact BES cyber systems. While we agree with the changes made to Section 6, subparts 6.1 and 6.2; the proposed language in subpart 6.3 is not sufficiently narrow. (See our response to question 1 above.)</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your comment. Please see our response to EEI, question 1.

**James Baldwin - Lower Colorado River Authority - 1**

**Answer** No

**Document Name**

**Comment**

LCRA believes that the current wording makes it unclear that only low impact BCS is applicable. Additionally, it is unclear if controls have to be implemented at the asset level.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.

**Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance**

**Answer** No

**Document Name**

**Comment**

LCRA believes that the current wording makes it clear that only low impact BCS is applicable. Additionally, it is unclear if controls have to be implemented at the asset level.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.

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

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
much more work is needed to sufficiently scope the low impact assets which will be considered in scope.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.	
<b>Brian Lindsey - Entergy - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Clarity is needed for when low impacts systems exist in conjunction with medium impact systems located at Medium BES Assets/Facilities. I.E. situations where there is a medium impact BES Asset/Facility that also contains low impact systems.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed. Cyber Assets identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.	
<b>Mike O'Neil - NextEra Energy - Florida Power and Light Co. - 1</b>	
<b>Answer</b>	No

<b>Document Name</b>	
<b>Comment</b>	
Please see NEE’s response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see response to question 1.	
<b>Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
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 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 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 6.3 completely.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6. Applying measures against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	

**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 the comments from the Edison Electric Institute (EEl) for questions #4.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see the response to EEl comments.

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

**Answer** No

**Document Name**

**Comment**

Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level.

Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed. Cyber Assets identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems. Further information can be found in CIP-003 TR section 3, reference model 7.

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

**Answer** No

**Document Name**

**Comment**

Section 6.3 should either reference Section 3.1 or somehow limit to only low impact BES cyber systems.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT updated language in Section 6 so that the statement “as established under Section 3” applies to all parts of Section 6.

**Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC**

**Answer** No

**Document Name**

**Comment**

Xcel Energy believes additional clarity could be established by adding verbiage to 6.3 that includes "as established in section 3"

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

**Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker**

<b>Answer</b>	No
---------------	----

<b>Document Name</b>	
----------------------	--

<b>Comment</b>
----------------

See EEI comment.

Likes 0	
---------	--

Dislikes 0	
------------	--

<b>Response</b>
-----------------

Thank you for your comment. Please see our response to EEI.

**Devon Tremont - Taunton Municipal Lighting Plant - 1**

<b>Answer</b>	No
---------------	----

<b>Document Name</b>	
----------------------	--

<b>Comment</b>
----------------

Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact.

Likes 0	
---------	--

Dislikes 0	
------------	--

<b>Response</b>
-----------------

Thank you for your comment. If low impact assets are mixed with medium impact assets then lows need to be highwater marked as medium or treated as distinct and separate systems.

**Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring**

<b>Answer</b>	No
---------------	----

<b>Document Name</b>	
<b>Comment</b>	
<p>The inclusion of ‘where such access has been established under Section 3’ appears to bring into scope electronic vendor remote access to Cyber Assets that <b>are not</b> low impact BES Cyber Systems, but on the same network as a low impact BES Cyber System based on the language of Section 3.1 ii ‘using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).’ This is due to the fact that CIP-003 uses ‘asset containing’ as a boundary.</p> <p>Please consider the following two options –</p> <p><b>Option 1:</b> Scope Section 6 specifically to Section 3.1 i, which would more accurately scope to only low impact BES Cyber Systems.</p> <p><i>Section 3.1 i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);</i></p> <p><b>Option 2:</b> Do not reference Section 3 or any part thereof, but include the following language in Attachment 1 Section 6 –</p> <p><i>‘between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).’</i></p> <p>6.1 One or more method(s) for determining electronic vendor remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);</p> <p>6.2 One or more method(s) for disabling electronic vendor remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside asset containing low impact BES Cyber System(s); and</p> <p>6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and out bound vendor communications between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).</p>	
Likes	0
Dislikes	0

**Response**

Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6.

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

**Answer** No

**Document Name**

**Comment**

There is confusion with the language used in Section 6 as to whether it pertains to the assets containing the low impact BES Cyber Systems (which may contain out of scope cyber systems) or the low impact BES Cyber Systems themselves.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.

**JT Kuehne - AEP - 6**

**Answer** No

**Document Name**

**Comment**

While AEP believes the proposed changes to the CIP-003 Standard are trending in the right direction overall, there was language struck through that we think adds clarity to the scope of the section. The aforementioned struck through language in Attachment 1 Section 6 is in bold below:

Section 6: Electronic Vendor Remote Access Security Controls: 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 vendor remote access **(including interactive and system-to-system access) to low impact BES Cyber Systems that includes:**

To provide a more clear understanding that the language in this section limits scope to low impact BES Cyber Systems, AEP recommends reinstating the language above that was struck from this revision.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6. Additionally, the SDT determined the language previously struck was in error and it has been reinstated.

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

**Answer**

No

**Document Name**

**Comment**

The lack of specificity in the “access to low impact BES Cyber Systems” verbiage could imply that an Entity will be required to document all vendor remote access or system-to-system access to the asset. This would include BES Cyber Systems, balance of plant for non-BCSs, and corporate business networks. The language in Section 6 states, “assets containing low impact BES Cyber System(s)” which does not limit the scope to only the “low impact BES Cyber Systems”. If the intent is to limit the scope to “low impact BES Cyber Systems” and not the “assets containing low impact BES Cyber Systems”, then significant changes would be warranted for CIP-002/CIP-003 to ensure low impact BES Cyber Systems are identified and that an Electronic Security Perimeter is established.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6. Section 3.1 does limit scope to low impact BES Cyber Systems contained within the low impact asset.

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

**Answer** No

**Document Name**

**Comment**

Comments: The lack of specificity in the “access to low impact BES Cyber Systems” verbiage could imply that an Entity will be required to document all vendor remote access or system-to-system access to the asset. This would include BES Cyber Systems, balance of plant for non-BCSs, and corporate business networks. The language in Section 6 states, “assets containing low impact BES Cyber System(s)” which does not limit the scope to only the “low impact BES Cyber Systems”. If the intent is to limit the scope to “low impact BES Cyber Systems” and not the “assets containing low impact BES Cyber Systems”, then significant changes would be warranted for CIP-002/CIP-003 to ensure low impact BES Cyber Systems are identified and that an Electronic Security Perimeter is established.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6. Section 3.1 does limit scope to low impact BES Cyber Systems contained within the low impact asset.

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

**Answer** Yes

**Document Name**

**Comment**

While NST agrees the Section 6 language limits the scope to low impact BCS, it is our opinion that it does not adequately define the types of in-scope vendor remote access. Do Sections 6.1 through 6.3 apply to vendor remote access via dial-up? Rather than simply use a blanket referral to Section 3 in Sections 6.1 and 6.2, Section 6 should refer to specific sub-parts of Section 3 (e.g., Section 3.1, Part i).

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6.

**Jamie Monette - Allele - Minnesota Power, Inc. - 1**

**Answer**

Yes

**Document Name**

**Comment**

No additional comments

Likes 0

Dislikes 0

**Response**

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

**Answer**

Yes

**Document Name**

**Comment**

<i>The NAGF has no comments.</i>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>George Brown - Acciona Energy North America - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this questi on.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to MRO NSRF.	
<b>Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
The MRO NSRF believes that the language is properly scoped.	
Likes 0	
Dislikes 0	

<b>Response</b>	
Thanks for your support.	
<b>Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
No comment	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Yes, the SDT has made the scope clear.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>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, Group Name Florida Municipal Power Agency (FMPA)</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Benjamin Winslett - Georgia System Operations Corporation - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mike Magruder - Avista - Avista Corporation - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Gerry Adamski - Cogentrix Energy Power Management, LLC - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
<b>Larry Heckert - Alliant Energy Corporation Services, Inc. - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>patricia ireland - DTE Energy - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

Comment	
Likes 0	
Dislikes 0	
Response	
<b>Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Scott Kinney - Avista - Avista Corporation - 3</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

<b>Susan Sosbe - Wabash Valley Power Association - 3</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Israel Perez - Salt River Project - 1,3,5,6 - WECC</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Fong 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; - Tim Kelley</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Jesus Sammy Alcaraz - Imperial Irrigation District - 1</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Glen Farmer - Avista - Avista Corporation - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Michelle Amarantos - APS - Arizona Public Service Co. - 5</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsey Mannion - ReliabilityFirst - 10</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Donald Lock - Talen Generation, LLC - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mike Marshall - IDACORP - Idaho Power Company - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes	0
Dislikes	0
<b>Response</b>	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	

<b>Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
No comment.	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>5. Do the examples in Attachment 2 Section 6 support your understanding of what is required in Attachment 1 Section 6? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification .</b>	
<b>Patricia Lynch - NRG - NRG Energy, Inc. - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Comments: Most of the suggested methods of achieving compliance go beyond the current requirements for low impact sites. Also, most of these methods require uniquely identified systems or assets, which is currently not required for low impact sites. If the intent of these proposed methods is to create a set of requirements similar to those for Medium Impact BES Cyber Systems, then the recommendation would be to eliminate CIP-003, R2 and incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s).</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<p>Thank you for your comment. The SDT believes implementation of the suggested methods can be applied at the system level and wouldn't require identification of individual Cyber Assets or Cyber Asset lists. The SDT does not believe the SAR allows this team to incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s) . Additionally, as currently structured, entities with low impact only are only subject to CIP-002 and CIP-003.</p>	
<b>Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment: Thank you</b>	

The examples provided support what is required in Attachment 1 Section 6. Clarification in the language used is suggested, along with an additional example for vendor machine to machine remote access:

Electronic Vendor Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation **AND EVIDENCE OF IMPLEMENTATION** showing:

? **DOCUMENTED** steps to preauthorize access **ALONG WITH AUTHORIZATION RECORDS**

? **CONFIGURATION OF** alerts generated by vendor log on;

? **PROCEDURES FOR THE USE OF VENDOR** session monitoring **AND SESSION MONITORING LOGS;**

? Security Information Management logging alerts; - **REDUNDANT TO #1, CAN BE REMOVED**

? **DOCUMENTED STEPS AND LOGS FOR** time-of-need session initiation;

? **DOCUMENTED STEPS AND LOGS FOR VENDOR REMOTE ACCESS** session recording;

? **DOCUMENTATION AND CONFIGURATION OF** system logs **SHOWING VENDOR REMOTE ACCESS CONNECTIONS**

? **DOCUMENTATION OF ELECTRONIC ACCESS CONTROL RULES PERMITTING INBOUND VENDOR MACHINE TO MACHINE COMMUNICATION;** or

? other operational, procedural, or technical controls.

For Section 6.2, documentation showing **THE PROCESS FOR:**

? disabling vendor remote access user or system accounts;

? disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active vendor remote access;

- ☐ disabling communications protocols (such as IP) used for systems which establish and/or maintain active vendor remote access;
- ☐ Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- ☐ administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access; or
- ☐ other operational, procedural, or technical controls.

For Section 6.3, documentation showing implementation of:

- ☐ Firewall policies **IMPLEMENTING MALICIOUS TRAFFIC INSPECTION**;
- ☐ Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- ☐ Virtual Private Network (VPN) hosts **IMPLEMENTING CONNECTION INSPECTION**;
- ☐ manual log reviews; or
- ☐ other operational, procedural, or technical controls.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT included examples of evidence in Attachment 2.

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

**Answer**

No

**Document Name**

**Comment**

Most of the suggested methods of achieving compliance go beyond the current requirements for low impact sites. Also, most of these methods require uniquely identified systems or assets, which is currently not required for low impact sites. If the intent of these

proposed methods is to create a set of requirements similar to those for Medium Impact BES Cyber Systems, then the recommendation would be to eliminate CIP-003, R2 and incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s).

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT believes implementation of the suggested methods can be applied at the system level and wouldn't require identification of individual Cyber Assets or Cyber Asset lists. The SDT does not believe the SAR allows for this team to incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s). Additionally, as currently structured, entities with low impact only are only subject to CIP-002 and CIP-003.

**Jesus Sammy Alcaraz - Imperial Irrigation District - 1**

**Answer** No

**Document Name**

**Comment**

Not clear if VPN connections established with support vendors fully adheres to requirement or additional steps are required such as an IDS/IPS.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. All connections established through Attachment 1 Section 3.1 are in scope for Section 6.

**Devon Tremont - Taunton Municipal Lighting Plant - 1**

**Answer** No

**Document Name**

**Comment**

Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – “administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access.” At attachment 1, Section 6 does not say “active vendor remote access.” Next that bullet is inconsistent with the first Attachment, 6.2 bullet – “disabling vendor remote access user or system accounts.”

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.

**Carl Pineault - Hydro-Quebec Production - 1,5**

**Answer**

No

**Document Name**

**Comment**

Agree in principle with these examples

Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – “administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access.” Attachment 1, Section 6 does not say “active vendor remote access.” Next that bullet is inconsistent with the first Attachment, 6.2 bullet – “disabling vendor remote access user or system accounts.”

Request consistency or clarification between CIP-003 and CIP-005. CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6 use different language than the proposed CIP-005, Part 2.5 Requirement – “Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).”

Likes 0

Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
<b>Gerry Adamski - Cogentrix Energy Power Management, LLC - 5</b>	
Answer	No
Document Name	
<b>Comment</b>	
Agree in principle with these examples	
Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – “administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access.” At Attachment 1, Section 6 does not say “active vendor remote access.” Next that bullet is inconsistent with the first Attachment, 6.2 bullet – “disabling vendor remote access user or system accounts.”	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
<b>Brian Lindsey - Entergy - 1</b>	
Answer	No
Document Name	
<b>Comment</b>	

Additional ephasis should be put on Programmatic non technical methods of allowance to clarify that processes can be leverage rather than purely technical methods.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Agree in principle with these examples	
Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – “administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access.” Attachment 1, Section 6 does not say “active vendor remote access.” Next, that bullet is inconsistent with the first Attachment, 6.2 bullet – “disabling vendor remote access user or system accounts.”	
Request consistency or clarification between CIP-003 and CIP-005. CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6 use different language than the proposed CIP-005, Part 2.5 Requirement – “Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).”	
Likes	0
Dislikes	0
<b>Response</b>	

Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.

**Daniel Gacek - Exelon - 1**

**Answer** No

**Document Name**

**Comment**

Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.

**Kinte Whitehead - Exelon - 3**

**Answer** No

**Document Name**

**Comment**

Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.

<b>Kimberly Turco - Constellation - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Constellation has elected to align with Exelon in response to this question.</p> <p>Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<p>Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.</p>	
<b>Alison Mackellar - Constellation - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Constellation has elected to align with Exelon in response to this question.</p> <p>Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.</p>	
Likes	0
Dislikes	0
<b>Response</b>	

Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.

**Deanna Carlson - Cowlitz County PUD - 5**

**Answer** No

**Document Name**

**Comment**

Cowlitz PUD supports the comments submitted by Utility Services Inc.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to Utility Services, Inc.

**Mike O'Neil - NextEra Energy - Florida Power and Light Co. - 1**

**Answer** No

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

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

**Answer** Yes

<b>Document Name</b>	
<b>Comment</b>	
Yes, the examples support our understanding of what is required.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
No comment	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Attachment 2 Section 6 includes multiple uses of ‘vendor remote access’ and ‘active vendor remote access.’ To ensure a consistent scope to Section 6 consider changing all to ‘**electronic vendor remote access.**’

disabling **vendor remote access user** or system accounts

disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing **active vendor remote access**

disabling communications protocols (such as IP) used for systems which establish and/or maintain **active vendor remote access**;

administrative control documentation listing the methods, steps, or systems used to disable **active vendor remote access**;

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT made clarifying changes to the draft language.

**Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker**

Answer

Yes

Document Name

**Comment**

See EEI comment.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to EEI.

<b>Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Xcel Energy believes that examples in Attachment 2 provide clarity to what is required in demonstrating compliance with Section 6.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>Donna Wood - Tri-State G and T Association, Inc. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Tri-State mostly agrees however, the example of Steps to Preauthorize is confusing and too open-ended.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
<b>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</b>	
<b>Answer</b>	Yes

<b>Document Name</b>	
<b>Comment</b>	
Energy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #5.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI, question 5.	
<b>Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
The MRO NSRF believes that the example are clear.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>George Brown - Acciona Energy North America - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to MRO NSRF.	
<b>Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
<i>The NAGF has no comments.</i>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
EEI agrees that Attachment 2, Section 6 examples support what is required under Attachment 1, Section 6.	
Likes 0	

Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>Benjamin Winslett - Georgia System Operations Corporation - 4</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
GSOC recommends that the language in Section 6.1 be revised to more closely mirror the language of CIP-005-7, R2.4, which would more clearly indicate the time frame and intent/activities to which the requirement and documentation should be focused.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
<b>Brian Evans-Mongeon - Utility Services, Inc. - 4</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
The examples listed for Section 6.2 include controls for disabling and controls for terminating remote access. In addition, these examples use the terms “vendor remote access” and “active vendor remote access” but do not use the “electronic vendor remote access” term used in Attachment 1. While we do not think the term “electronic vendor remote access” should be used at all, there should be consistency throughout the document and preferably, consistency throughout the CIP Standards.	
Likes	0

Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
<b>Jamie Monette - Allete - Minnesota Power, Inc. - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
No additional comments	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
PGE supports the survey response provided by EEI.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	

<b>Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
NST has no comment.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>Daniel Mason - Portland General Electric Co. - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
PGE supports the survey response provided by EEI.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Richard Jackson - U.S. Bureau of Reclamation - 1,5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your support.	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Mike Marshall - IDACORP - Idaho Power Company - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	

<b>Donald Lock - Talen Generation, LLC - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>JT Kuehne - AEP - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Lindsey Mannion - ReliabilityFirst - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Michelle Amarantos - APS - Arizona Public Service Co. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Glen Farmer - Avista - Avista Corporation - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Fong 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; - Tim Kelley</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Israel Perez - Salt River Project - 1,3,5,6 - WECC</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Susan Sosbe - Wabash Valley Power Association - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>Scott Kinney - Avista - Avista Corporation - 3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1</b>	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Thank you for your support.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>patricia ireland - DTE Energy - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Larry Heckert - Alliant Energy Corporation Services, Inc. - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
Thank you for your support.	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Mike Magruder - Avista - Avista Corporation - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your support.	
<b>Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>James Baldwin - Lower Colorado River Authority - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your support.	
<b>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, Group Name Florida Municipal Power Agency (FMPA)</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your support.	
<b>Russell Noble - Cowlitz County PUD - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your support.	
<b>John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	

No comment.	
Likes 0	
Dislikes 0	
<b>Response</b>	

**6. 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.**

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

**Answer** No

**Document Name**

**Comment**

NST 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 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, NST 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 and on the number of facilities where controls may need to be applied.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.

**Russell Noble - Cowlitz County PUD - 3**

**Answer** No

**Document Name**

**Comment**

Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to Utility Services, Inc.	
<b>Jamie Monette - Allele - Minnesota Power, Inc. - 1</b>	
Answer	No
Document Name	
<b>Comment</b>	
Until additional clarity is provided on the scope and intent of the proposed modifications, the overall cost is difficult to ascertain.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT believes the proposed draft clarifies the scope and intent of the standard modifications.	
<b>Alison Mackellar - Constellation - 5</b>	
Answer	No
Document Name	
<b>Comment</b>	
Constellation has elected to align with Exelon in response to this question.	
Registered Entities could incur significant costs implementing considering the Low Cyber Asset inventory included.	

Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to Exelon.	
<b>Kimberly Turco - Constellation - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Constellation has elected to align with Exelon in response to this question.	
Registered Entities could incur significant costs implementing considering the Low Cyber Asset inventory included.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to Exelon.	
<b>Kinte Whitehead - Exelon - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Registered Entities would incur significant costs implementing, considering the Low asset inventory included in the scope.	
Likes	0
Dislikes	0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes and configuration.

**Daniel Gacek - Exelon - 1**

**Answer**

No

**Document Name**

**Comment**

Registered Entities would incur significant costs implementing, considering the Low asset inventory included in the scope.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes and configuration.

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

**Answer**

No

**Document Name**

**Comment**

The expansion of the requirement to detect suspicious malicious communication to systems that may not have routable communication and to systems that are not at a Control Center, as is required for high and medium impact, imposes costs that are not consistent with the risks as determined by previous Standard Drafting Teams.

Furthermore we believe the SDT is only accounting for the cost of the equipment that would be responsible for performing the tasks of Section 6. While this is one cost to consider, there may be additional resources required to allow for implementation of such technology

including but not limited to additional staffing, training, or other equipment that would allow a SIM/SEM/SIEM or IDS/IPS to have visibility.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT updated language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6. Please see the TR for additional information.

The SDT understands the cost of implementing a new requirement includes equipment as well as cost of training or staffing employees.

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

**Answer** No

**Document Name**

**Comment**

Due to supply chain issues and other geopolitical factors, it is difficult to determine the cost effectiveness of implementin g this standard.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

**James Baldwin - Lower Colorado River Authority - 1**

**Answer** No

**Document Name**

**Comment**

There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. This could pose fiscal challenges to entities.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
<b>Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name</b> ACES Standard Collaborations	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
This is very dependent on how an entity chose to implement it's low impact electronic access controls, the size of the organization, and if the organization has medium or high impact Control Centers.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
<b>Teresa Krabe - Lower Colorado River Authority - 5, Group Name</b> LCRA Compliance	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	

There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. This could pose fiscal challenges to entities.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
<b>Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF</b>	
Answer	No
Document Name	
<b>Comment</b>	
Any low impact related changes are likely to lead to significant scope creep and potentially many underlying, unknown costs that will be incurred.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The SDT realizes there are unknowns with implementation and has increased the implementation plan to 36 months to account for this.	
<b>Mike Magruder - Avista - Avista Corporation - 1</b>	
Answer	No
Document Name	
<b>Comment</b>	

The changes limit the scope of what traffic must be monitored, but the technology and resources needed to conduct the monitoring remains the same.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
<b>George Brown - Acciona Energy North America - 5</b>	
Answer	No
Document Name	
<b>Comment</b>	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this questi on.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to MRO NSRF.	
<b>Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF</b>	
Answer	No
Document Name	
<b>Comment</b>	

<p>The MRO NSRF has concerns about the potential of ineffective costs. Due to recent supply chain issues, industry-wide staffing shortages, and other geopolitical factors the cost of implementation of the Requirements is at a much higher risk than what would normally be expected. Higher than expected costs may result in the need for a longer or adaptive implementation timeline.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<p>Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes ,and configuration. The SDT realizes there are unknowns with implementation and has increased the implementation plan to 36 months to account for this.</p>	
<b>Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro</b>	
Answer	No
Document Name	
<b>Comment</b>	
<p>Although the cost may differ between entities, BC Hydro's assessment is that the impact may change based on understanding &amp; clarity of terms and scope of application. As outlined in BC Hydro's comments to Question 1 above, CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. However, the requirement in CIP-003-X Section 6.3 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 out of scope.</p> <p>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.</p>	
Likes	0
Dislikes	0
<b>Response</b>	

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.

**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**

Making this a requirement on all low impact BES Cyber Systems would be extremely expensive because new equipment must be installed at each low location to monitor for remote vendor access, allow for the ability to terminate sessions and detect malicious code. It would be more cost effective to create a risk-based approach that would target those low impact BES Cyber Systems that could have the most potential impact on the BES.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.

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

**Answer** No

**Document Name**

**Comment**

There are many entities that have a large amount of low impact sites that are in remote locations and struggle with limited bandwidth that will be impacted. With the recent supply chain and staffing issues you will have higher than normal costs to implement these requirements.

Likes	0
-------	---

Dislikes	0
----------	---

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.

**Larry Heckert - Alliant Energy Corporation Services, Inc. - 4**

Answer	No
--------	----

Document Name	
---------------	--

**Comment**

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes	0
-------	---

Dislikes	0
----------	---

**Response**

Thank you for your comment. Please see our response to MRO NSRF.

**Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC**

Answer	No
--------	----

Document Name	
---------------	--

**Comment**

Xcel Energy is concerned with meeting the demands of section 6 in a cost effective manner at this time. World events have created issues with supply chain and receiving the needed products to perform activities required in the standard in a timely and cost effective manner. The vast number of low impact sites as compared to high and medium sites will cause a sudden surge in demand and cause prices to rise dramatically. The standard drafting team should take these issues into consideration in their implementation plan to spread costs and demand for products across and longer span of time.

Likes	0
-------	---

Dislikes	0
----------	---

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The SDT realizes there are unknowns with implementation and has increased the implementation plan to 36 months to account for this.

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

Answer	No
--------	----

Document Name	
---------------	--

**Comment**

AEPCO is signing on to ACES comments below.

ACES comments: This is very dependent on how an entity chose to implement it's low impact electronic access controls, the size of the organization, and if the organization has medium or high impact Control Centers.

Likes	0
-------	---

Dislikes	0
----------	---

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.

<b>Scott Kinney - Avista - Avista Corporation - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
The changes limit the scope of what traffic must be monitored, but the technology and resources needed to conduct the monitoring remains the same.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
<b>Susan Sosbe - Wabash Valley Power Association - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
This is very dependent on how an entity chose to implement it's low impact electronic access controls, the size of the organization, and if the organization has medium or high impact Control Centers.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	

<b>Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Due to supply chain issues and other geopolitical factors, it is difficult to determine the cost effectiveness of implementing this standard.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
<b>Glen Farmer - Avista - Avista Corporation - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
The changes limit the scope of what traffic must be monitored, but the technology and resources needed to conduct the monitoring remains the same.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
<b>Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1</b>	

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Depending on the solution(s) determined by NIPSCO, cost would most likely be a factor to purchase the equipment and resources necessary to achieve the goal of securing vendor remote access.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
The scope should be narrowed to just where the risk exists as opposed to a broad swath of assets. The way it is written it implies that all communications need to be monitored to determine malicious communications through vendor remote access.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The team also believes the modifications have limited the scope of Section 6.	

**Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato**

**Answer** No

**Document Name**

**Comment**

Due to supply chain issues and other geopolitical factors, it is difficult to determine the cost effectiveness of implementing this standard.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.

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

**Answer** No

**Document Name**

**Comment**

These modifications, as they are currently written, could be misinterpreted, which would result in a significant expansion of scope of the CIP-003 Attachment 1 requirements and prove detrimental to a cost-effective approach. Please reference previously provided comments for additional detail.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The team also believes that the modifications have limited the scope of Section 6.

**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**

Thank you for your comment. The SDT does not believe the SAR allows this team to incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s). Additionally, as currently structured, entities with low impact only are only subject to CIP-002 and CIP-003.

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

**Answer** No

**Document Name**

**Comment**

Comments: These modifications, as they are currently written, could be misinterpreted, which would result in a significant expansion of scope of the CIP-003 Attachment 1 requirements and prove detrimental to a cost-effective approach. Please reference previously provided comments for additional detail.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The team also believes the modifications have limited the scope of Section 6.

**Deanna Carlson - Cowlitz County PUD - 5**

Answer

No

Document Name

Comment

Likes 0

Dislikes 0

**Response**

**Benjamin Winslett - Georgia System Operations Corporation - 4**

Answer

Yes

Document Name

Comment

<p>GSOC is concerned that compliance with Section 6, as proposed, may require a significant investment of resources, specifically that such investment is beyond what is applied to protect high or medium impact BES cyber assets despite the fact that such investment may not yield commensurate reliability and security benefits.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<p>Thank you for your comment. Applying measures to mitigate against malicious communications to Low Impact BCS and not all Mediums is addressed in the TR.</p>	
<p><b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b></p>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<p><b>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, Group Name Florida Municipal Power Agency (FMPPA)</b></p>	
Answer	Yes
Document Name	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Gerry Adamski - Cogentrix Energy Power Management, LLC - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Israel Perez - Salt River Project - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Fong 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; - Tim Kelley</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Jesus Sammy Alcaraz - Imperial Irrigation District - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Michelle Amarantos - APS - Arizona Public Service Co. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsey Mannion - ReliabilityFirst - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>JT Kuehne - AEP - 6</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Donald Lock - Talen Generation, LLC - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Mike Marshall - IDACORP - Idaho Power Company - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Daniel Mason - Portland General Electric Co. - 6</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
N/A	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
No comment.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<i>GO/GOPs will need more information to adequately assess the cost-effectiveness of the proposed approach.</i>	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your comment.	
<b>Carl Pineault - Hydro-Qu?bec Production - 1,5</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
No comment	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>patricia ireland - DTE Energy - 4</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<i>We will need more information to adequately assess the cost-effectiveness of the proposed approach</i>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter</b>	
<b>Answer</b>	

<b>Document Name</b>	<a href="#">2020-03_Supply_Chain_Lows_Unofficial_Comment_Form_02252022 Presentation FINAL COMMENTS v2.docx</a>
<b>Comment</b>	
To be “cost effective”, this implies the proposed modification to the CIP-003 standard can be absorbed with existing company staff and minor procedure adjustment. Based on the high volume of Low Impact Cyber System locations and varied configurations that we have in our service territory (approximately 10 times the level of CIP Medium Impact locations), this is not a cost-effective change. Additional staff and procedures will be required to monitor this level of detail to meet the requirements of CIP-003.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Texas RE does not have comments on the question.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
<b>Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF</b>	

<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
SIGE will not provide a response to the cost effectiveness of the proposed changes to CIP-003-x.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
A longer implementation timeline would offer more cost effectiveness. This would allow industry to spread their investments and capital purchases.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT increased the implementation plan to 36 months based on industry feedback.	

**7. The SDT is proposing an 18-month implementation plan for Attachment 1, Section 6.1 and 6.2. The proposed implementation time frame for Attachment 1, Section 6.3 is 24-months. Would these proposed timeframes 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**

Thank you for your comment. The SDT has changed the implementation plan to 36 months.

**Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato**

**Answer** No

**Document Name**

**Comment**

BHE expects implementation of Section 6.3 to require the purchase of a significant amount of new equipment. Hundreds of Registered Entities will all be purchasing intrusion detection systems at the same time, and within a short deliverable window to allow time for

installation, resulting in even greater supply chain issues. Please consider adding something like the following to the implementation plan to address this potential issue: “If the Responsible Entity encounters significant supply chain issues, the Responsible Entity may request an extension from the Regional Entity.” While this would need additional details developed, it would provide the industry with assurance that supply chain issues outside of their control would not result in non-compliance. An example of an extension might be equal to the time between placing orders for needed equipment and receiving said orders. BHE also requests NERC consider ways to work with equipment manufacturers to try to address the increased demand for this equipment.

Likes	0
Dislikes	0

**Response**

Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.

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

<b>Answer</b>	No
---------------	----

<b>Document Name</b>	
----------------------	--

**Comment**

Sections 6.1 and 6.2 will not have equivalent language for Mediums without ERC until CIP-005-8 R2.4 and R2.5 are adopted. Therefore, BPA recommends that implementation of these sections should be aligned with the passage of CIP-005-8 to avoid entities having to monitor their Low assets but not their Mediums without ERC and/or Dialup.

Section 6.3 has no current equivalent language in CIP-005-8 (nor any other standards) for Medium impact BES Cyber Systems except at Control Centers. Until then, entities will be expected to detect malicious communications at certain Low assets but none of their Medium assets outside of a control center. This is a significant gap; BPA recommends that the drafting team delay Section 6.3 until CIP-005 is expanded to include Mediums outside of Control Centers.

Likes	0
Dislikes	0

<b>Response</b>	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
<b>Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
After further consideration, we believe that a 36 month implementation timeline would be most appropriate for incorporating all the revisions in Project 2020-03. This will allow for proper installation, testing and documentation of new controls across a large inventory of sites and assets. This timeline would also be more feasible given the current supply chain challenges across industry.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
The expansion of scope for vendor remote access monitoring and malicious communication monitoring may require new technology to be implemented within the program. The implementation for said technology for a large utility will require a longer implementation than 24 months.	
Likes	0

Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1</b>	
Answer	No
Document Name	
<b>Comment</b>	
36 months minimum as additional staff or staff augmentation would have to be employed as there would be a significant amount of design, planning, testing, and finally, deployment of solutions to the affected assets in the field.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Michelle Amarantos - APS - Arizona Public Service Co. - 5</b>	
Answer	No
Document Name	
<b>Comment</b>	
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 Sections 6.1 and 6.2, in addition to Section 6.3. 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
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Jesus Sammy Alcaraz - Imperial Irrigation District - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Due to supply chain constraints on security equipment we believe an additional 12 months should be included or an exception were procurements happens within that time frame to adhere compliance.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
BHE expects implementation of Section 6.3 to require the purchase of a significant amount of new equipment. Hundreds of Registered Entities will all be purchasing intrusion detection systems at the same time, and within a short deliverable window to allow time for installation, resulting in even greater supply chain issues. Please consider adding something like the following to the implementation plan to address this potential issue: "If the Responsible Entity encounters significant supply chain issues, the Responsible Entity may request an extension from the Regional Entity." While this would need additional details developed, it would provide the industry with assurance	

that supply chain issues outside of their control would not result in non-compliance. An example of an extension might be equal to the time between placing orders for needed equipment and receiving said orders. BHE also requests NERC consider ways to work with equipment manufacturers to try to address the increased demand for this equipment.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.

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

Answer

No

Document Name

**Comment**

A 24 month implementation is desirable due to budget, supply chain, and resources to implement solutions for SRP's Generation fleet.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT has changed the implementation plan to 36 months.

**Susan Sosbe - Wabash Valley Power Association - 3**

Answer

No

Document Name

**Comment**

Again this is very dependent on the size of the entity, if the entity has medium or high impact BES Cyber Systems, if the entity has medium or high impact BES Cyber Systems at Control Centers, how many low impact BES Cyber Systems the entity has, and if supply chain will play a role in delaying the implementation of the controls for entities. Because of potential supply chain issues and new technology implementation, there needs to be allowances at least for Attachment 1, Section 6.3, to allow entities more time to implement, the required control, if necessary.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT has changed the implementation plan to 36 months.

**Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker**

Answer

No

Document Name

**Comment**

See EEI comment.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to EEI.

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

Answer

No

Document Name

**Comment**

AEPCO is signing on to ACES comments below.

ACES comments: Again this is very dependent on the size of the entity, if the entity has medium or high impact BES Cyber Systems, if the entity has medium or high impact BES Cyber Systems at Control Centers, how many low impact BES Cyber Systems the entity has, and if supply chain will play a role in delaying the implementation of the controls for entities. Because of potential supply chain issues and new technology implementation, there needs to be allowances at least for Attachment 1, Section 6.3, to allow entities more time to implement, the required control, if necessary.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT has changed the implementation plan to 36 months.

**Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1**

Answer

No

Document Name

**Comment**

PNM supports EEL comments regarding the implementation timeframe for 6.3 to be extended to 36-months if the scope of 6.3 is not sufficiently narrowed as mentioned in the comments for question 1.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to EEL.

**Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC**

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Xcel Energy is concerned with meeting the implementation demands of section 6 within the proposed timeline identified in the implementation plan. World events have created issues with supply chain and obtaining the needed products and staff to perform activities required in the standard in a timely manner. The vast number of low impact sites as compared to high and medium sites will cause a sudden surge in demand and cause prices to rise dramatically. Additionally, an industry-wide staffing shortage will slow efforts to implement and maintain newly procured products. The standard drafting team should take these issues into consideration in the implementation plan to spread costs and demand for products and staff across and longer span of time.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<p>Thank you for your comment. The SDT changed the implementation plan to 36 months.</p>	
<b>Larry Heckert - Alliant Energy Corporation Services, Inc. - 4</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Alliant Energy supports the comments submitted by the MRO NSRF.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<p>Thank you for your comment. Please see our response to MRO NSRF.</p>	

<b>Donna Wood - Tri-State G and T Association, Inc. - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
As mentioned in Question 6, many entities have large amount of low impact sites that are in remote locations and struggle with limited bandwidth which makes procurement, and implementation of new hardware and software difficult. There is the other challenge of the recent supply chain and staffing issues that will also impact implementation timelines. The supply chain being taxed all at once by utilities to meet the short timeline should must be taken into consideration.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>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</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEl) for questions #7.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEl.	

<b>Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>BC Hydro recommends a longer implementation plan, e.g. more than ~ 36 months considering the cost and scope impact as identified in comments to Questions 1 and 4 above. Once the clarity of terms and definitions is obtained as identified in comments to Questions 1 and 4, BC Hydro will be in a better position to provide an alternate detailed implementation plan to meet the target completion deadline.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<p>Thank you for your comment. The SDT has changed the implementation plan to 36 months.</p>	
<b>Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>The MRO NSRF anticipates the procurement and implementation of new software, hardware, and associated services needed to detect vendor’s malicious communications to be particularly challenging given recent supply chain issues, industry-wide staffing shortages, and other geopolitical factors. Registered Entities across North America will all be attempting to procure needed solutions in a relatively small window of time. This will create a deficit of supply with increased demand and will drive up costs. That, along with current staffing shortages and geopolitical events, may produce scenarios that will prevent a responsible entity from meeting the effective date set in the approved implementation plan. The MRO NSRF suggests the SDT align with NERC legal staff to allow for a provision in the implementation plan that would provide an opportunity for entities to request extensions based on the aforementioned factors.</p>	
Likes	0

Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.	
<b>George Brown - Acciona Energy North America - 5</b>	
Answer	No
Document Name	
<b>Comment</b>	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this questi on.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to MRO NSRF.	
<b>Mike O’Neil - NextEra Energy - Florida Power and Light Co. - 1</b>	
Answer	No
Document Name	
<b>Comment</b>	
<ul style="list-style-type: none"> <li>• NextEra Energy requests consideration of a 36-month implementation period due to a large number of sites (in the hundreds) requiring assessment and potentially new equipment and/or process implementation. The work must be planned and typically will be scheduled with planned maintenance and scheduled generation outages.</li> <li>• The last few years the supply chain has adversely impacted maintenance including staffing and is expected to impact the implementation.</li> </ul>	

- Entities may need to evaluate and update vendor, supplier, customer and other agreements and contracts.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT has changed the implementation plan to 36 months.

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

**Answer**

No

**Document Name**

**Comment**

Given the uncertainty regarding the exact scope of implementation across low impact and all vendor communications it is hard to believe the 18 months will be sufficient timing.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT has changed the implementation plan to 36 months.

**Brian Lindsey - Entergy - 1**

**Answer**

No

**Document Name**

**Comment**

There could be additional needs for technology purposes which would create funding needs based on funding cycles and implementation. Strongly recommended to increase all sections to a 24 mth implementation.

Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Teresa Krabe - Lower Colorado River Authority - 5, Group Name</b> LCRA Compliance	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. Implementation of new technology takes time and careful consideration. Additionally, current supply chain challenges may pose an additional risk to effectively implementing.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name</b> ACES Standard Collaborations	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Again this is very dependent on the size of the entity, if the entity has medium or high impact BES Cyber Systems, if the entity has medium or high impact BES Cyber Systems at Control Centers, how many low impact BES Cyber Systems the entity has, and if supply chain will play a role in delaying the implementation of the controls for entities. Because of potential supply chain issues and new	

technology implementation, there needs to be allowances at least for Attachment 1, Section 6.3, to allow entities more time to implement, the required control, if necessary.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.

**James Baldwin - Lower Colorado River Authority - 1**

**Answer**

No

**Document Name**

**Comment**

There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. Implementation of new technology takes time and careful consideration. Additionally, current supply chain challenges may pose an additional risk to effectively implementing.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT has changed the implementation plan to 36 months.

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

**Answer**

No

**Document Name**

**Comment**

EEl appreciates the two-phase implementation plan for Attachment 1, Section 6 and supports the proposed 18-month implementation plan for subparts 6.1 and 6.2. However, we do not agree that an additional 6 months to complete subpart 6.3 is adequate, particularly given the current proposed language could be interpreted to mean all low impact BES Cyber System communication. Moreover, if the current language is not narrowed consistent with a risk-based approach it may be a significant challenge for some entities to complete this work in 36 months. EEl previously noted that there will be substantial work to complete 6.3 and companies are also facing significant supply chain issues/delays to secure materials necessary to implement these changes. For these reasons, the implementation plan should be at a minimum of 36 months.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.

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

**Answer**

No

**Document Name**

**Comment**

NVE expects implementation of Section 6.3 to require the purchase of a significant amount of new equipment. Hundreds of Registered Entities will all be purchasing intrusion detection systems at the same time, and within a short deliverable window to allow time for installation, resulting in even greater supply chain issues. Please consider adding something like the following to the implementation plan to address this potential issue: "If the Responsible Entity encounters significant supply chain issues, the Responsible Entity may request an extension from the Regional Entity." While this would need additional details developed, it would provide the industry with assurance that supply chain issues outside of their control would not result in non-compliance. An example of an extension might be equal to the time between placing orders for needed equipment and receiving said orders. NVE also requests NERC consider ways to work with equipment manufacturers to try to address the increased demand for this equipment.

Likes 0

Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.	
<b>Benjamin Winslett - Georgia System Operations Corporation - 4</b>	
Answer	No
Document Name	
<b>Comment</b>	
Given the potential impact of expanded scope of Section 6.3, GSOC would respectfully request a 24 month implementation period given the current state of global supply chain lead times.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Daniel Gacek - Exelon - 1</b>	
Answer	No
Document Name	
<b>Comment</b>	
One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes 0	
Dislikes 0	

<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Kinte Whitehead - Exelon - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Kimberly Turco - Constellation - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Constellation has elected to align with Exelon in response to this question.	
One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes	0
Dislikes	0

<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Alison Mackellar - Constellation - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Constellation has elected to align with Exelon in response to this question.	
One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Jamie Monette - Allete - Minnesota Power, Inc. - 1</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Until additional clarification is provided on the scope and intent of the proposed changes, it's unclear if the drafted implementation timelines are sufficient to implement the requirements.	
Likes	0
Dislikes	0

<b>Response</b>	
Thank you for your comment. Clarifying changes have been made to the draft language and the implementation plan has been set to 36 months.	
<b>Ryan Olson - Portland General Electric Co. - 5, Group Name</b> PGE Group 2	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
PGE supports the survey response provided by EEI.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Russell Noble - Cowlitz County PUD - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Cowlitz PUD supports the comments submitted by the Bonneville Power Administration (BPA).	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. Please see our response to BPA.	

<b>Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
NST believes the time required 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 and on the number of facilities where controls may need to be applied. NST recommends a 24-month implementation time frame for all of Attachment 1, Section 6 requirements.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Daniel Mason - Portland General Electric Co. - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>We would rather have one date of 24 months for the whole thing. Simpler to track and entities are going to need the time for various reasons. Some that don't have IDS capabilities at all their sites will have to order and receive and then implement a lot of equipment at a lot of sites. The 6.1 and 6.2 can be shorter for TO/TOPs that just have substations, or for those with only control centers. With the wide diversity of vendor situations out there on everything from a small solar to a string of wind turbines to a large Generation facility and all matters of variety of vendor arrangements and support, the timeframe and implementation plan is not simple. We do not want to make the assumption that 6.3 is 'hard' and needs more time and 6.1 and 6.2 are 'easier' and can be done quicker. In some cases, it might be the opposite. Whatever the maximum implementation time is, give that to everyone.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<p>Thank you for your comment. The SDT has changed the implementation plan to 36 months.</p>	
<b>Deanna Carlson - Cowlitz County PUD - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Patricia Lynch - NRG - NRG Energy, Inc. - 5</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Comments: These timeframes are sufficient assuming that a significant expansion in scope isn't being proposed. Please reference previously provided comments for additional detail.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT has made clarifying changes and set the implementation plan to 36 months.	
<b>Martin Sidor - NRG - NRG Energy, Inc. - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
These timeframes are sufficient assuming that a significant expansion in scope isn't being proposed. Please reference previously provided comments for additional detail.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT has made clarifying changes and set the implementation plan to 36 months.	
<b>Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
<b>Carl Pineault - Hydro-Quebec Production - 1,5</b>	
Answer	Yes
Document Name	
Comment	
Consider large-scale supply chain and implementation issues. If all entities request supplies at the same time, what will be the supply chain impact?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
Answer	Yes
Document Name	
Comment	

If all examples in Attachment 2 are ever required then we believe that additional time above the 18 months may be required.	
Likes	0
Dislikes	0
<b>Response</b>	
Thanks you for your comment. The SDT has changed the implementation plan to 36 months. The examples within Attachment 2 are just examples and is not a comprehensive list.	
<b>Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
<i>The NAGF has no comments.</i>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Consider large-scale supply chain and implementation issues. If all entities request supplies at the same time, what will be the supply chain impact?	

Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
<b>Brian Evans-Mongeon - Utility Services, Inc. - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
The ability for entities to apply these control may be limited by the availability of equipment and the vendors qualified to install them. The SDT should request that NERC provide information on the expected number of substations that may be required to implement these controls. It may be necessary to include an automatic extension of the time allowed for implementation, if necessary, equipment and personnel to perform the installation are not available.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.	
<b>Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0

Dislikes 0	
<b>Response</b>	
<b>Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Mike Marshall - IDACORP - Idaho Power Company - 1	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Donald Lock - Talen Generation, LLC - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>JT Kuehne - AEP - 6</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF</b>	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lindsey Mannion - ReliabilityFirst - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
<b>Glen Farmer - Avista - Avista Corporation - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Fong 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; - Tim Kelley</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Devon Tremont - Taunton Municipal Lighting Plant - 1</b>	
<b>Answer</b>	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Scott Kinney - Avista - Avista Corporation - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>patricia ireland - DTE Energy - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Gerry Adamski - Cogentrix Energy Power Management, LLC - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Mike Magruder - Avista - Avista Corporation - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>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, Group Name Florida Municipal Power Agency (FMPA)</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
Answer	
Document Name	
<b>Comment</b>	
Texas RE does not have comments on the question.	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<p>If scope of this standard is tightened to what FE believes is the spirit of the standard, we feel we could follow the proposed implementation plan. As it is written, we feel the vagueness of the draft leaves ambiguity and would require a longer implementation plan to fulfill our obligation.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<p>Thank you for your comment. The SDT changed the implementation plan to 36 months and updated the draft language with clarifying changes.</p>	
<b>John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<p>No comment.</p>	
Likes 0	
Dislikes 0	

## Response

<b>8. Provide any additional comments on the standard and technical rationale document for the standard drafting team to consider, if desired.</b>	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
These 'low' requirements as written seem to be more stringent than what highs and mediums have to comply with today. Highs and Mediums have to determine 'active' sessions and have a method to disable remote access. That is far easier than determining what constitutes malicious inbound and outbound communications.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
<b>Daniel Mason - Portland General Electric Co. - 6</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
N/A	
Likes 0	
Dislikes 0	

Response	
<p><b>Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh</b></p>	
<b>Answer</b>	
<b>Document Name</b>	
Comment	
<p>NST believes it is short-sighted to add a new requirement to CIP-003 for malicious communications detection that is limited to vendor remote access only. Advocates for this limitation seem to be ignoring the possibility a Responsible Entity's own remote computer systems could be compromised by attackers and used to deliver malware to BES Cyber Systems (BCS) at BES assets containing low impact BCS. In addition, NST believes that limiting the scope of monitoring and detecting to only vendor remote access either may not be practical or may result in sub-optimal designs that would need to be updated should monitoring and detecting requirements be expanded in the future. Given the likely time, effort, and expense associated with implementing a solution for malicious code detection (using IDS or similar technology), we think it only makes sense to require it for all remote access. NST also notes that in its recent NOPR proposing "Internal Network Security Monitoring" requirements for high and medium BES Cyber Systems, FERC indicated it is interested in the possibility of applying "INSM" requirements to low impact, as well. This suggests to us that while FERC might approve the current set of proposed supply chain revisions to CIP-003, were they to be approved by industry ballot and the NERC board, they might also direct NERC to further modify CIP-003 to apply malicious communications detection requirements to any remote access that uses routable protocols outside BES assets containing low impact BCS.</p>	
Likes 0	
Dislikes 0	
Response	
<p>Thank you for your comments. The SDT had several conversations about this topic with NERC compliance and legal staff. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access. The SDT believes the drafted standard meets the current objective from the NERC BOT and SAR. While looking "forward" to future requirements and/or</p>	

potential standards that might be considered, it is beyond this teams current scope, which is focused solely on supply chain and vendor’s access.

**Russell Noble - Cowlitz County PUD - 3**

Answer

Document Name

Comment

Cowlitz PUD supports the comments submitted by Utility Services Inc.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to Utility Services, Inc.

**Romel Aquino - Edison International - Southern California Edison Company - 3**

Answer

Document Name

Comment

See Comments submitted by the Edison Electric Institute.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to EEI.

**Selene Willis - Edison International - Southern California Edison Company - 5**

<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
See Comments submitted by the Edison Electric Institute.” with your ballot.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Please see our response to EEI.	
<b>Alison Mackellar - Constellation - 5</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
SDT should consider defining the term “Electronic Vendor” in the NERC defined Glossary of Terms.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT modified the language to remove this term.	
<b>Kimberly Turco - Constellation - 6</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	

SDT should consider defining the term “Electronic Vendor” in the NERC defined Glossary of Terms.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT modified the language to remove this term.	
<b>Kinte Whitehead - Exelon - 3</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
What is meant by ‘ <b>Electronic</b> Vendor’? Currently it’s not a defined term, SDT should consider making this a NERC defined glossary term.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT modified the language to remove this term.	
<b>Daniel Gacek - Exelon - 1</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
What is meant by ‘ <b>Electronic</b> Vendor’? Currently it’s not a defined term, SDT should consider making this a NERC defined glossary term.	
Likes	0

Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT modified the language to remove this term.	
<b>Brian Evans-Mongeon - Utility Services, Inc. - 4</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
All proposed controls should be limited to only low impact BES Cyber Systems as opposed to assets containing low impact BES Cyber Systems.	
The proposed control for detecting malicious communication should be limited to:	
<ol style="list-style-type: none"> <li>1. Only low impact BES Cyber Systems using a routable protocol to communicate across the asset boundary and,</li> <li>2. Only Control Centers (to align with CIP-005-7 R1.5)</li> </ol>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT made changes to reduce the scope based on only those communications that are established through Attachment 1, Section 3.1. The SDT asserts that the SAR applies to all low impact facilities as identified in CIP-002.	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	

For future reference, request redline to last approved since that shows the true SDT proposed updates.

Recommend updating R1.2.6 by removing “Electronic” from “Electronic vendor remote access security controls.” The security concern is vendor remote access.

Recommend updating Attachment 1 by removing “Electronic” from “Electronic vendor” for consistency with Requirement R1.2.6

Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “detecting known or suspected malicious communications for both inbound and outbound vendor communications.” 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6’s Applicable Systems says “Medium impact BCS at Control Centers” 6.3 applies to all vendor communications, not just Control Centers.

Recommend updating Attachment 2 by removing “Electronic” from “Electronic vendor” for consistency with Requirement R1.2.6

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT made clarifying changes regarding the comment about “electronic vendor”. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.

**John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway**

**Answer**

**Document Name**

**Comment**

No comment.

Likes 0

Dislikes 0

<b>Response</b>	
<b>Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
The Technical Rationale document had a footnote reference to the term vendor as used in CIP-013 that was removed. NVE found it useful and requests that the footnote be reinstated.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The TR has been updated.	
<b>Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
In the proposed Draft 2 of CIP-003-x, the undefined term “Electronic Vendor” has been used eleven times (including within Section 6 of Attachment 1). It is unclear what is meant by the use of this term and if this term is to remain within this Reliability Standard, the SDT should provide needed clarification through the Technical Rationale.	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your comment. The SDT has removed the term.	
<b>Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
We would like to thank the SDT for their efforts and allowing the industry to participate in the drafting process.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<i>The NAGF membership recommends that the SDT consider providing reference architecture diagram(s) similar to previous reference model provided in CIP-003.</i>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The Project 2016-02 team is preserving the reference documents that were in the GTB of CIP-003-8 in TR documents going forward. The diagrams that reference section 3 still apply to this draft of the standard and any communication crossing those boundaries are still appropriate.	

<b>Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
No additional comments at this time.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brian Lindsey - Entergy - 1</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
NA	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1</b>	
<b>Answer</b>	
<b>Document Name</b>	

## Comment

- Please provide redline to last approved since that shows the true SDT proposed updates.
- Please apply NEE’s response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6 to the standard and technical rationale document.
- Page 4 “ The SDT agreed to retain Section 3 and establish Section 6 to address vendors and low impact electronic remote access,” change to “**The SDT agreed to retain Section 3 and establish Section 6 to address low impact vendor electronic remote access,**”
- Page 5:
  - “establish and disable electronic vendor remote access.” to be “**establish and disable vendor electronic remote access.**”
  - “low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.” to be “low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active **vendor electronic remote access** sessions are initiated; and (3) disable active **vendor electronic remote access** when necessary.”
- Attachment 1 Section 6 Part 6.1 – Determining **Vendor Electronic Remote Access**
  - “associated with malicious communications and electronic vendor remote access.” to be “**associated with malicious communications and vendor electronic remote access.**”
- Attachment 1 Section 6 Part 6.2 – Disabling **vendor electronic remote access**
  - Enhanced visibility into electronic vendor remote access and the ability to terminate electronic vendor remote access could mitigate such a vulnerability. The obligation in Section 6.2 requires that entities have a method to disable electronic vendor remote access.” to be “**Enhanced visibility into vendor electronic remote access** and the ability to terminate **vendor electronic remote access** could mitigate such a vulnerability. The obligation in Section 6.2 requires that entities have a method to disable **vendor electronic remote access.**”

- Page 6
- Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications for **vendor electronic remote access**

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The team made clarifying changes to the draft language of the standard and updated the TR.

**George Brown - Acciona Energy North America - 5**

**Answer**

**Document Name**

**Comment**

Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this questi on.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see the response to MRO NSRF.

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

**Answer**

**Document Name**

**Comment**

The MRO NSRF would like to thank the Standard Drafting Team, NERC Staff and all other contributors for their work on this project.

Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Gerry Adamski - Cogentrix Energy Power Management, LLC - 5</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<p>For future reference, request redline to last approved since that shows the true SDT proposed updates.</p> <p>Recommend updating R1.2.6 by removing “Electronic” from “Electronic vendor remote access security controls.” The security concern is vendor remote access.</p> <p>Recommend updating Attachment 1 by removing “Electronic” from “Electronic vendor” for consistency with Requirement R1.2.6</p> <p>Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “detecting known or suspected malicious communications for both inbound and outbound vendor communications.” 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6’s Applicable Systems says “Medium impact BCS at Control Centers” 6.3 applies to all vendor communications, not just Control Centers. The low requirement may encompass email, phone, and or mail communications from vendors, because of the vague language used.</p> <p>Recommend updating Attachment 2 by removing “Electronic” from “Electronic vendor” for consistency with Requirement R1.2.6</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	

Thank you for your comment. The SDT made updates to clarify the language in the standard. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.

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

**Answer**

**Document Name**

**Comment**

BC Hydro acknowledges the effort and hard work SDT put into putting these complex changes to CIP-003-X. As identified in comments to Questions 1 to 4 above. The definitions of terms and clarity of application with some specific industry use case examples will help providing a more clear understanding and likely result in a faster and appropriate approvals of these proposed changes.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The team asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.

**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**

**Document Name**

**Comment**

Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #8.

Likes 0

Dislikes 0

Response	
Thank you for your comment. Please see our response to EEI.	
<b>Carl Pineault - Hydro-Quebec Production - 1,5</b>	
<b>Answer</b>	
<b>Document Name</b>	
Comment	
<p>For future reference, request redline to last approved since that shows the true SDT proposed updates.</p> <p>Recommend updating R1.2.6 by removing “Electronic” from “Electronic vendor remote access security controls.” The security concern is vendor remote access.</p> <p>Recommend updating Attachment 1 by removing “Electronic” from “Electronic vendor” for consistency with Requirement R1.2.6</p> <p>Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “detecting known or suspected malicious communications for both inbound and outbound vendor communications.” 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6’s Applicable Systems says “Medium impact BCS at Control Centers” 6.3 applies to all vendor communications, not just Control Centers.</p> <p>Recommend updating Attachment 2 by removing “Electronic” from “Electronic vendor” for consistency with Requirement R1.2.6</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. The SDT made updates to clarify the language in the standard. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	

<b>Larry Heckert - Alliant Energy Corporation Services, Inc. - 4</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Alliant Energy appreciates the Standard Drafting Team's work on this project.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Xcel Energy would like to thank the drafting team for their diligent work and bringing forward language to address the concerns identified by the NERC BOT.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>patricia ireland - DTE Energy - 4</b>	
<b>Answer</b>	

<b>Document Name</b>	
<b>Comment</b>	
We remain concerned that the CIP-003 Attachment 1, Section 6.3 requirement for malicious communication places a heavier compliance burden on low impact assets than High and Medium, as delineated in CIP-005 (2.4 and 2.5). Simply extending the the implementation timeframe for this requirement does not address that basic inconsistency.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
<b>Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Thank you to the SDT for their efforts and allowing AEPCO to participate in the drafting process.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Scott Kinney - Avista - Avista Corporation - 3</b>	
<b>Answer</b>	
<b>Document Name</b>	

**Comment**

My intended vote for this ballot was negative based on the comments provided in this survey. However due to technical issues with the voting platform while casting my vote it is shown as affirmative. If possible please replace my affirmative vote with a negative vote.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Votes cannot be changed in the system. If you experience issues with the system in the future, please reach out 24-48 hours prior to the comment period/ballot close so we can look into it.

**Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker**

Answer

Document Name

**Comment**

See EEI comment.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. Please see our response to EEI.

**Susan Sosbe - Wabash Valley Power Association - 3**

Answer

Document Name

**Comment**

We would like to thank the SDT for their efforts and allowing the industry to participate in the drafting process.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Texas RE continues to have the following additional recommendations for the SDT:	
<ul style="list-style-type: none"> <li>• Include language for (1) software integrity and authenticity, (2) information 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.</li> <li>• 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.</li> <li>• Include controls for encrypted vendor remote access sessions, which is consistent with CIP-005 Requirement R2.</li> </ul>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment. The SDT believes the proposed language meets the requirement of our current SAR. If additional requirements as discussed above were included, it would extend outside the scope of the approved SAR.	
<b>Israel Perez - Salt River Project - 1,3,5,6 - WECC</b>	
<b>Answer</b>	

<b>Document Name</b>	
<b>Comment</b>	
Will inventory lists now be required for Low Impact sites? Based on the current requirements, is it safe to assume that cloud electronic access controls are acceptable for vendor remote access into low impact sites?	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT asserts that nothing that was added in Section 6 changes the scope of assets that entities were already required to create based on the others sections of Attachment 1.	
<b>Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
The Technical Rationale document had a footnote reference to the term vendor as used in CIP-013 that was removed. BHE found it useful and requests that the footnote be reinstated.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The SDT updated the TR to reflect the changes in the current draft.	
<b>Devon Tremont - Taunton Municipal Lighting Plant - 1</b>	
<b>Answer</b>	
<b>Document Name</b>	

**Comment**

The most concerning to us is Attachment 1, Section 6.3 in which the term "detecting" known or suspected malicious communications for vendors is used. The term "detecting" is unclear to us. We are unsure if this would require continuous monitoring of the vendor's session, or if it is simply intended to at least manually review the vendor's session after the fact. Is the intent to provide constant real-time monitoring, which would be costly and time consuming?

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The current draft language is intended to be risk-based to allow entities flexibility in defining their plans and then implementing the plan as designed.

**Jesus Sammy Alcaraz - Imperial Irrigation District - 1**

**Answer**

**Document Name**

**Comment**

With the consideration of the FERC NOPR. Additional architecture diagrams should be illustrated for a possible IDS/IPS implementation similar to when EAC under section 3 there were guidance architecture diagrams.

Likes 0

Dislikes 0

**Response**

Thank you for your comment. The Project 2016-02 team is preserving the reference documents that were in the GTB of CIP-003-8 in TR documents going forward. The diagrams that reference section 3 still apply to this draft of the standard and any communication crossing those boundaries are still appropriate.

**Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring**

<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
In the Technical Rational, first sentence in the foreward, consider using language consistent with Section 6. Change 'electronic remote vendor access' to 'electronic vendor remote access.'	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The TR has been updated to reflect the current draft language.	
<b>Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
No comment	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller</b>	
<b>Answer</b>	
<b>Document Name</b>	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato</b>	
Answer	
Document Name	
<b>Comment</b>	
The Technical Rationale document had a footnote reference to the term vendor as used in CIP-013 that was removed. BHE found it useful and requests that the footnote be reinstated.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment. The TR has been updated to reflect the current draft language.	
<b>Richard Jackson - U.S. Bureau of Reclamation - 1,5</b>	
Answer	
Document Name	
<b>Comment</b>	

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**

Thank you for your comment.

**End of Report**