NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2019-03 Cyber Security Supply Chain Risks | CIP-005-7, CIP-010-4, & CIP-013-2 (Draft 3)
Comment Period Start Date:	7/28/2020
Comment Period End Date:	9/10/2020
Associated Ballot:	2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 AB 3 ST

There were 59 sets of responses, including comments from approximately 135 different people from approximately 85 companies representing 10 of the 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, please 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, you can contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry's concerns about recursive requirements (‘hall of mirrors’). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

5. Provide any additional comments 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
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISONE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Ali Miremadi	CAISO	2	WECC
Douglas Webb	Douglas Webb		MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
CMS Energy - Consumers Energy Company	Jeanne Kurzynowski	3,4,5	RF	Consumers Energy Company	Jeanne Kurzynowski	Consumers Energy Company	1,3,4,5	RF
					Jim Anderson	Consumers Energy Company	1	RF
					Karl Blaszkowski	Consumers Energy Company	3	RF
					Theresa Martinez	Consumers Energy Company	4	RF
					David Greyerbiehl	Consumers Energy Company	5	RF
ACES Power Marketing	Jodirah Green	1,3,4,5,6		ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
			MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC			Cooperative, Inc.		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
FirstEnergy - FirstEnergy Corporation	Julie Severino	1		FirstEnergy	Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Mark Garza	FirstEnergy - FirstEnergy Corporation	4	RF
DTE Energy - Detroit Edison Company	Karie Barczak	3		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Randy MacDonald	NB Power Corporation	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, 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

N&ST believes there are several problems with proposed requirement R3 as presently written

- It addresses “authenticated vendor-initiated remote connections” without explicitly establishing a requirement for authentication, nor does it provide a working definition of a “remote connection.”
- Part 3.2’s mandate to control the ability of a vendor whose connection has been terminated to reconnect creates a consistency problem. There is no comparable requirement in Requirement R2 for vendor remote connections to BES Cyber Systems and PCAs.
- A second inconsistency is created by using the term, “remote connection” in R3, whereas the term, “remote access” is used in R2.

N&ST recommends the following changes:

- Move R3’s proposed Parts 3.1 and 3.2 to R2 and eliminate R3. N&ST sees no need to address vendor remote access to applicable systems in two separate, top-level requirements.
- Modify the “applicability” language in those two Parts to say, for example:
    - “EACMS and PACS:
    - associated with High Impact BES Cyber Systems, and
    - not located within any of the Responsible Entity’s Electronic Security Perimeter(s).”
        - NOTE: 2nd bullet is taken verbatim from the Glossary definition of IRA
- Add an explicit requirement to use at least one form of authentication.

- Consider adding language, taken from the existing IRA definition, that that clarifies "vendor remote access" originates from "Cyber Assets used or owned by vendors, contractors, or consultants." The SDT may want to consider adding this to existing R2 Parts 2.4 and 2.5, as well.
- Change “remote connection” to “remote access”
- The proposed requirement to control vendor reconnection should either be eliminated or added to existing R2 Part 2.5.

Likes 1	Central Hudson Gas &amp;amp; Electric Corp., 1, Pace Frank
Dislikes 0	

Response

Thank you for your comment. During the second ballot, the SDT realized how problematic this was after industry expressed concern about Parts 2.4 and 2.5 moving into R3, and effectively creating a recursive requirement (also known as the “Hall of mirrors”) that would have required use of Intermediate System for vendor-initiated remote access to an EACMS. Since an Intermediate System is an EACMS by definition, this unintended consequence could have created a potential never-ending condition and an impossibility to comply, so we took that very seriously. The SDT listened to these concerns, and resolved this by restoring Parts 2.4 and 2.5 to the original currently approved CIP-005-6 language and Applicable Systems, and we not proposing any modifications to those two parts. Instead, the SDT refocused on the FERC Order and the SAR scope and is proposing R3 be dedicated specifically to EACMS and PACS associated to high and medium impact BES Cyber Systems. Here you see the redline for the newly proposed parent Requirement R3, where the SDT: Added EACMS address the directive in FERC Order 850, and Added PACS to address the recommendation in the NERC Cyber Security Supply Chain Risks Report.

Industry was also concerned about ambiguity in the phrase ‘vendor remote access’, and how it could lead to varied interpretations that an attempt to establish a session ‘***to***’ an EACMS that is later denied ‘***by***’ the EACMS could be considered ‘access’. A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.

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

Answer	No
Document Name	

Comment

ACES does not agree with the use of “authenticated” and “remote connections” in R3.

R3 without the word authenticated, covers all vendor connections .. CIP-004 R4.1 already requires access management for EACMS and PACS and CIP-007 R5.1 requires methods to enforce authentication. Further, as discussed on the project 2019-03 webinar, unauthenticated remote access is already addressed by the CIP standards. Lastly, an authorized remote connection can be made without being authenticated. Thus an authorized malicious insider could easily craft a denial of service without ever being completely authenticated. Removing the word “authenticated” would put more emphasis on **all** vendor connections and increases the security objective of R3. Suggested language:

“Have one or more method(s) to determine vendor initiated remote access.”

Secondly, the CIP standards have always used the NERC defined term: Interactive Remote Access and or remote access vs what is in the draft “remote connections”. ACES suggests using language consistent with existing standards. Without defining “remote connections”, it makes the requirement vague and could be interpreted differently. Suggested language:

“Have one or more method(s) to terminate vendor initiated remote access and control the ability to reconnect.”

Likes 0	
Dislikes 0	

Response: Thank you for your response. The SDT agrees with this perspective on CIP-004 and CIP-007; however, the changes that were made were specific to external vendor-initiated remote access.

The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is <u>not</u> prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

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

Answer	No
Document Name	

Comment

BPA proposes the SDT eliminate references to “vendor.” The requirements should apply to any active remote sessions.

Proposed change to R2.4:

Have one or more methods for determining detecting active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

Proposed change to R2.5:

Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

Likes 0	
Dislikes 0	

Response:

Thank you for your comment. During the second ballot, the SDT realized how problematic this was after industry expressed concern about Parts 2.4 and 2.5 moving into R3, and effectively creating a recursive requirement (also known as the “Hall of mirrors”) that would have required use of Intermediate System for vendor-initiated remote access to an EACMS. Since an Intermediate System is an EACMS by definition, this unintended consequence could have created a potential never-ending condition and an impossibility to comply, so we took that very seriously. The SDT listened to these concerns, and resolved this by restoring Parts 2.4 and 2.5 to the original currently approved CIP-005-6 language and Applicable Systems, and we not proposing any modifications to those two parts. Instead, the SDT refocused on the FERC Order and the SAR scope and is proposing R3 be dedicated specifically to EACMS and PACS associated to high and medium impact BES Cyber Systems. Here you see the redline for the newly proposed parent Requirement R3, where the SDT: Added

EACMS address the directive in FERC Order 850, and Added PACS to address the recommendation in the NERC Cyber Security Supply Chain Risks Report.

Industry was also concerned about ambiguity in the phrase ‘vendor remote access’, and how it could lead to varied interpretations that an attempt to establish a session ‘***to***’ an EACMS that is later denied ‘***by***’ the EACMS could be considered ‘access’. A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

Restoring R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language is fine, but the language in R3 is unclear. It’s not clear what “authenticated vendor-initiated” remote connections are. The intent seems clear, and the security necessity is warranted, but it is not clear why using something like “Have one or more method(s) for determining authorized vendor-initiated remote access connections” is not used. What value does using “authenticated” vendor-initiated remote access connections add? Why is “Remote Connections” used instead of “Remote Access” since R3 is “Vendor Remote Access”? What is considered a remote connection? Does a remote connection include both system to system communication and remote access? Is a remote connection from outside of an entities corporate network or is it a remote connection from inside an entities network but behind a firewall and using some remote access client?

Likes 0

Dislikes 0

Response: Thank you for your comment. The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.

- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device. - This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment. The SDT determined to not define the term “Remote” because it is context dependent (i.e., external to your corporate network versus external to your ESP, etc.).	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
If the requirements are technically the same, as it appears, then the new scope should be added to Parts 2.4 and 2.5. However, we believe the SDT was attempting to resolve some ambiguity that currently exists around what is vendor remote access. We commend the SDT for this effort, and request they clarify the existing requirements (parts 2.4 and 2.5). Specifically, vendor remote access should be defined or somehow clarified that it only includes access where the vendor's personnel or system has direct access and ability to control the session. Having IRA and system-to-system listed as examples, but not an all-inclusive list, would also be helpful.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. During the second ballot, the SDT realized how problematic this was after industry expressed concern about Parts 2.4 and 2.5 moving into R3, and effectively creating a recursive requirement (also known as the “Hall of mirrors”) that would have required use of Intermediate System for vendor-initiated remote access to an EACMS. Since an Intermediate System is an EACMS by definition, this unintended consequence could have created a potential never-ending condition and an impossibility to comply, so we took that very seriously. The SDT listened to these concerns, and resolved this by restoring Parts 2.4 and 2.5 to the original currently	

approved CIP-005-6 language and Applicable Systems, and we not proposing any modifications to those two parts. Instead, the SDT refocused on the FERC Order and the SAR scope and is proposing R3 be dedicated specifically to EACMS and PACS associated to high and medium impact BES Cyber Systems. Here you see the redline for the newly proposed parent Requirement R3, where the SDT: Added EACMS address the directive in FERC Order 850, and Added PACS to address the recommendation in the NERC Cyber Security Supply Chain Risks Report. Industry was also concerned about ambiguity in the phrase ‘vendor remote access’, and how it could lead to varied interpretations that an attempt to establish a session ‘***to***’ an EACMS that is later denied ‘***by***’ the EACMS could be considered ‘access’. A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
The SDT should provide guidance or clarify the role or function of Intermediate Systems in context of providing electronic access to EACMS and PACS located within an ESP vs outside an ESP. If the SDT intends to *exclude* Interactive Remote Access (IRA) requirements for EACMS or PACS in CIP-005-7 R3.1 and R3.2, it should clarify that an intermediate system is not required to electronically access an EACMS and PACS located outside an ESP. However, if the EACMS or PACS is located within the ESP, the entity is required to utilize an Intermediate System for electronic access. This brings into scope all CIP-005 R2 requirements. Without guidance, entities may interpret that an Intermediate System is never required for the vendor IRA to EACMS or PACS - even though they may exist within an ESP. The SDT did not use the defined term IRA in R3.1 and R3.2, but if an EACMS or PACS is inside an ESP and the vendor remote access meets the IRA definition, does SDT allow a vendor IRA to the EACMS or PACS inside an ESP without the IRA requirements of CIP-005 R2?	

The SDT could consider putting all vendor remote access sub-requirements in one requirement – 3.0.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. It is not within the scope of the 2019-03 SAR for the SDT to resolve regional interpretation inconsistencies regarding dual classification of EACMS and/or PACS installed inside an ESP and the varied implications on Intermediate System need. The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC’s Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC’s Compliance & Enforcement team, who can assess and unify audit interpretation.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
Agree with leaving R2 as is. Disagree with need for a R3. Actually, the SDT should be providing us with a cost/benefit justification for change.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. During the second ballot, the SDT realized how problematic this was after industry expressed concern about Parts 2.4 and 2.5 moving into R3, and effectively creating a recursive requirement (also known as the “Hall of mirrors”) that would have required use of Intermediate System for vendor-initiated remote access to an EACMS. Since an Intermediate System is an EACMS by definition, this unintended consequence could have created a potential never-ending condition and an impossibility to comply, so we took that very seriously. The SDT listened to these concerns, and resolved this by restoring Parts 2.4 and 2.5 to the original currently	

approved CIP-005-6 language and Applicable Systems, and we not proposing any modifications to those two parts. Instead, the SDT refocused on the FERC Order and the SAR scope and is proposing R3 be dedicated specifically to EACMS and PACS associated to high and medium impact BES Cyber Systems. Here you see the redline for the newly proposed parent Requirement R3, where the SDT: Added EACMS address the directive in FERC Order 850, and Added PACS to address the recommendation in the NERC Cyber Security Supply Chain Risks Report.

Industry was also concerned about ambiguity in the phrase ‘vendor remote access’, and how it could lead to varied interpretations that an attempt to establish a session ‘***to***’ an EACMS that is later denied ‘***by***’ the EACMS could be considered ‘access’. A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.

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

We thought a CIP Modification SDT goal was to remove this language to assist the coming virtualization updates.

Request clarification on why CIP-005 R2 Parts 2.4 & 2.5 use the phrase “vendor remote access” while CIP-013 R1 Part 1.2.6 uses the phrase “vendor-initiated remote access” We are concerned that omitting “initiated” may introduce unintended requirements in CIP-005.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Project 2019-03 had a FERC directive to meet and the 2016-02 team will make conforming changes to the approved CIP-005-7 to enable virtualization going forward while maintaining backwards compatibility.

In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC greatly appreciates the drafting team's efforts and thoughtful approach regarding this proposal. However, it is concerned that the splitting of these requirements creates significant potential for very different compliance obligations for the different classes of assets while attaining the same or similar cyber security protections as would be garnered solely with either set of requirements. More specifically, the differentiation between the requirements for PACS and EACMSs and the assets to which access is sought is likely to cause confusion as well as increase the potential for differing interpretations of compliance and "double jeopardy." That the proposed split of requirements would likely provide little or no additional security benefit, while being unduly burdensome for entities, creates additional concerns for responsible entities as they try to focus their resources on those activities that will have a net effect of enhancing security.

GSOC understands that industry comments have driven these proposed changes, and agrees that valid concerns have been presented (e.g., the hall of mirrors). In its response to question #2, GSOC proposes an approach to addressing these previous concerns and comments that will allow a return to a simpler approach for the requirements generally. We respectfully recommend that the SDT consider utilizing alternative approaches such as are proposed below, e.g., definition revision, to allow the requirements to more clearly and succinctly meet the Commission directives regarding EACMS and PACS. This simpler approach to address concerns will facilitate a reversion of the requirement language to the initial proposal where EACMSs and PACs were added as applicable systems for the existing requirements.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT considered the proposed revisions suggested in question 2 and determined that the proposed definition recreates the hall of mirrors issue. The SDT asserts that requirement R2 and R3 are mutually exclusive requirements with mutually exclusive systems and does not create double jeopardy.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
please reference Marty Hostler, Northern California Power Agency, comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to Marty Hostler.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with restoring R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and adding R3 for EACMS and PACS.	
Likes 0	
Dislikes 0	

Response
Thank you for your comment.

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

We recommend that view only access by a vendor is not considered IRA, nor vendor remote access.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. This comment has been turned over to NERC compliance for review.

Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy

Answer	Yes
Document Name	

Comment

To separate the remote access from the vendor remote access, FirstEnergy would respectfully suggest that the currently drafted R2 Parts 2.4 and 2.5 are reorganized to become R3 Parts 3.1 and 3.2. Subsequently, the currently drafted R3 3.1 and 3.2 become Parts 3.3 and 3.4.

Likes 0	
Dislikes 0	

Response Thank you for your comment. The changes you are requesting were contained in draft 2 of the standards and was voted down by industry due to the recursive nature of the requirements that it introduced. This new requirement R3 is mutually exclusive from R2 and its parts.	
Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with comments submitted separately by Tom Breene of WEC	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to WECC.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment, please see response to EEI's comments.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE agrees with the proposed approach to restore the CIP-005-7 Requirements R2 Parts 2.4 and 2.5. However, ISO-NE recommends the use of consistent "vendor remote access" or "vendor-initiated remote connections" for both Requirement R2 Part 2.4 and R2.5 and the Requirement R3 Parts 3.1 and 3.2.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E believes this is the appropriate modifications in-line with the industry comments made to the second Comment & Ballot. The restoration of the P2.4 and P2.5, along with the modifications made in Requirement R3 more clearly eliminate the potential interpretation that could have resulted in recursive requirements noted in Question 2 below.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
MidAmerican supports EEI commnets	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to EEI.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Thank you for your comment, please see response to EEI.

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

Answer	Yes
Document Name	

Comment

Cleco agrees with EEI comments.

Likes 0	
Dislikes 0	

Response

Thank you for your comment, please see response to EEI.

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

NV Energy supports EEI's comments on Q1:

"While EEI supports the changes made by the SDT, which addressed prior EEI member comments related to CIP-005-7 Requirement R2 Parts 2.4 and 2.5, we ask the SDT to consider revising “vendor remote access” to “vendor initiated remote access” or provide clarification why they believe that all vendor remote access should be considered under Parts 2.4 and 2.5.

EEI supports the current proposed draft language for Requirement R3."

In addition, NVE supports the revision of "vendor remote access" to "vendor initiated remote access" due to current conflicting interpretations of P2.5 and 2.5 and CIP-005-6 by Regional Entities. WECC has identified videoconferences (initiated by the Entity) as "vendor remote access", which does not align with industry interpretation (NATF, other Regional Entities), so further clarification of this action would provide more clarity for future interpretations.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.

It is not within the scope of the 2019-03 SAR for the SDT to resolve regional interpretation inconsistencies. The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC’s Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC’s Compliance & Enforcement team, who can assess and unify audit interpretation.

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

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

Likes 0	
Dislikes 0	

Response

Thank you for your comment, please see response to EEI.

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks

Answer	Yes
Document Name	

Comment

The ISO/RTO Council Standards Review Committee (IRC SRC) [1] supports the restoration of CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original, currently approved CIP-005-6 language and Applicable Systems.

In addition, we agree with the addition of Requirement R3, Parts 3.1 and 3.2 to focus on the directive in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report to have one or more methods to determine and be able to terminate vendor-initiated remote connections to EACMS and PACS.

That said, the IRC SRC requests the Standard Drafting Team (SDT) provide additional clarity around the term “authenticated” to align and memorialize what was verbally (and non-binding) presented by the SDT in the Project 2019-03 webinar (timestamp 9:00 – 10:00 of 37:24) on August 5, 2020.

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is <u>not</u> prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer	Yes
Document Name	

Comment

Westar Energy and Kansas City Power & Light, the Evergy companies, support and incorporate by reference the Edison Electric Institute’s response to Question 1.

Likes 0	
Dislikes 0	

Response

Thank you for your comments, please see response to EEI.

Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

The CAISO supports the ISO/RTO Council Standards Review Committee comments below.

ISO/RTO Council Standards Review Committee (IRC SRC)[1] supports the restoration of CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original, currently approved CIP-005-6 language and Applicable Systems.

In addition, we agree with the addition of Requirement R3, Parts 3.1 and 3.2 to focus on the directive in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report to have one or more methods to determine and be able to terminate vendor-initiated remote connections to EACMS and PACS.

That said, the IRC SRC requests the Standard Drafting Team (SDT) provide additional clarity around the term “authenticated” to align and memorialize what was verbally (and non-binding) presented by the SDT in the Project 2019-03 webinar (timestamp 9:00 – 10:00 of 37:24) on August 5, 2020.

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is <u>not</u> prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

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

Answer	Yes

Document Name	
Comment	
Requirements R2 and R3 have subtly different language (e.g. "disable" vs. "terminate" and "vendor-initiated") in addition to different applicability. Matching the language or updating the language so the same processes developed for R2 could be used for R3 would reduce regulatory burden.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT understand the subtle differences in the language and because of the differences in the assets in the applicability section, the SDT concluded that the differences in language were required so as to not introduce unintended consequences i.e. hall of mirrors effect. The SDT has documented rationale in the Technical Rationale document associated with CIP-005-7.	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Requirements R2 and R3 have subtly different language (e.g. "disable" vs. "terminate" and "vendor-initiated") in addition to different applicability. Matching the language or updating the language so the same processes developed for R2 could be used for R3 would reduce regulatory burden	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT understand the subtle differences in the language and because of the differences in the assets in the applicability section, the SDT concluded that the differences in language were required so as to not introduce unintended consequences i.e. hall of mirrors effect. The SDT has documented rationale in the Technical Rationale document associated with CIP-005-7.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees with restoring CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language, as well as addressing vendor remote access for EACMS and PACS in the newly formed Requirement R3. However, Texas RE is concerned that in addressing vendor remote access for EACMS and PACS, the Standard Drafting Team (SDT) has elected to use the term “authenticated vendor-initiated remote connections.” Texas RE notes that “authenticated vendor-initiated remote connections” is not presently defined. As such, the introduction of such a term may create additional ambiguity, particularly around what constitutes an “authenticated” vendor-initiated remote connection. Texas RE suggests that the SDT could address this concern by using clarifying that such access includes “Interactive Remote Access and system-to-system remote access” as presently defined in the current and proposed Requirement 2.4 and 2.5.	

Texas RE suggests the “hall of mirrors” concern could be better addressed by adding language to Requirement R3 that excludes Intermediate Systems for EACMS and PACS in the applicability section. Alternatively, the SDT could revise the definition of Interactive Remote Access to clarify this point.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

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

Likes 0	
Dislikes 0	

Response

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

Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry's concerns about recursive requirements (‘hall of mirrors’). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC appreciates the SDT's efforts to remove the “hall of mirrors” concerns, but suggests a return to the simpler approach for the requirements as discussed in its response to question #1. To support this reversion, GSOC recommends the following revision to the definition of EACMS to address the ‘Hall of Mirrors” concern:Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. **This includes Intermediate Systems and does not include those systems that only perform electronic access control or electronic access monitoring to or from other EACMSs.** GSOC suggests that incorporating the recommended revision above will address the “hall of mirrors” concern, which will allow the SDT to revert the proposed language to the simpler approach described in question 1 above and eliminate the need to create multiple requirements to address the same or similar security and access controls/objectives.	
Likes 0	
Dislikes 0	
Response Thank you for your comments. At this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT believes that the suggested definition would recreate the hall of mirrors issue which was addressed by creating R3.1 and R3.2.	

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

We agree with the SDT on removing the hall of mirrors. But the "authentication" clarification below is necessary.

We request clarification of authenticating. The Technical Rationale, page 11 under R3, says this "authenticating" means authenticating the connection, not authenticating the user. This clarification should be in this Standard. This clarification is needed to avoid confusion with CIP-004.

We request clarification on the distinction between "connection" and "access."

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT recommends reviewing the Technical Rationale, which states the below:

- A 'connection' is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- "Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to 'how' authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

CIP-005-7 Requirement R3 picks up after the user or device has already used its authorized vendor remote access to make an authenticated connection. The CIP-005-7 Requirement R3 controls focus on the connection itself and not the access.

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

Answer	No
Document Name	

Comment

Tri-State does not agree with the new terminology, as it is open to interpretation.

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

Response

Thank you for your comment. The SDT has prepared implementation guidance and technical rationale to assist industry.

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

Answer	No
Document Name	

Comment

BPA believes the SDT should address this issue with requirements aimed at securing the management plane of EACMS rather than continuing down the path of perimeter-based security and bastion hosts (jump boxes and DMZs) as a sole protection for protected enclaves. This would clarify the recursive effect of “intermediate systems for intermediate systems ad nauseam.” This recursive effect problem seems related to the history of previous drafting teams endlessly debating whether a “packet to a port” is “access.” There may be a connection (a term with no recognized and easily specified meaning in NIST); however, a connection is generally not considered “authenticated” because “authentication” occurs at a different layer of the OSI model. Authentication is associated with sessions (ephemeral or time limited and specific to an interactive or programmed action) rather than connections (which are typically permanently configured, filtered, and existing at least in potential all the time, more associated with physical infrastructure as well).

There is a problem buried in current discussions of “authenticated” or ”provisioned” access that will continue to encourage entities to avoid more advanced technology such as next generation firewalls with role-based permissions. Currently, standard and extended access control lists based upon source, destination, and port/protocol contain no “authentication” mechanism. Filtering based upon source and destination is not a means of authentication. Therefore, a “packet to a port” to an EACMS that is allowed by source IP is a connection, and lacks authentication, but does not constitute “access.” Industry typically does not refer to “unauthenticated connections” but rather to authenticated or unauthenticated “sessions.” The SDT should conform to this more-common terminology because it tracks better with security principles and the technical implementations of authentication mechanism. Establishing a “session” to an EACMS to manage/configure it would constitute “access”, and require authentication and other security controls securing the management plane. Under this construct, requirements can be crafted to avoid the recursive perimeter protection problem.

Entities could design a solution where any unauthenticated connection, using only an IP source address to authorize passing the traffic, would avoid the requirement to detect active sessions entirely. This perverse incentive/loophole must be discouraged.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Project 2016-02 SDT will make conforming changes once Project 2019-03 completes. CIP-005-7 Requirement R3 picks up after the user or device has already used its authorized vendor remote access to make an authenticated connection. The CIP-005-7 Requirement R3 controls focus on the connection itself and not the access.

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

Answer	No
Document Name	

Comment

While N&ST agrees that recursive requirements should be avoided, we believe the proposed changes do not address the possibility of an EACMS or PACS being located within an established Electronic Security Perimeter with sufficient clarity. N&ST recommends, in addition to moving R3 Parts 3.1 and 3.2 to R2 and eliminating R3, that "Applicability" language for those two Parts be modified to clarify that they apply to EACMS and PACS that are not located within any of the Responsible Entity's Electronic Security Perimeters.

Likes 0	

Dislikes 0	
Response Thank you for your comment. It is not within the scope of the 2019-03 SAR for the SDT to resolve regional interpretation inconsistencies regarding dual classification of EACMS and/or PACS installed inside an ESP and the varied implications on Intermediate System need. The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC's Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC's Compliance & Enforcement team, who can assess and unify audit interpretation.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
please reference Marty Hostler, Northern California Power Agency, comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to Northern California Power Agency.	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
The CAISO supports the ISO/RTO Council Standards Review Committee comments below.	

The IRC SRC supports the removal of references to IRA and the undefined term “system to system” from CIP-005-7, requirement R3, Parts 3.1 and 3.2 to clarify that Intermediate Systems are optional and not required for EACMS or PACS.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Westar Energy and Kansas City Power & Light, the Evergy companies, support and incorporate by reference the Edison Electric Institute’s response to Question 2.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	

Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
The IRC SRC supports the removal of references to IRA and the undefined term “system to system” from CIP-005-7, requirement R3, Parts 3.1 and 3.2 to clarify that Intermediate Systems are optional and not required for EACMS or PACS.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	

It is important that the SDT clarify the applicable in-scope systems based on their risk to the Bulk Electric System and further clarify the role of Intermediate Systems and their capabilities and functions.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. In the last posting the SDT believes that the requirements are clarified based on risk by reverting back to Requirement R2.4 and R2.5 and adding Requirement R3 for EACMS and PACS.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	

Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
MidAmerican supports EEI comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the modification and that it does help clarify the condition of elimination of a recursive requirement (hall of mirrors) and the Requirement is for the EACMS and PACS, and not the BCS,

Likes 0	
Dislikes 0	

Response

Thank you for your comment.

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

Answer	Yes
Document Name	

Comment

ISO-NE agrees with the proposed approach to restore the CIP-005-7 Requirements R3. However, ISO-NE recommends the use of consistent “vendor remote access” or “vendor-initiated remote connections” for both Requirement R2 Part 2.4 and R2.5 and the Requirement R3 Parts 3.1 and 3.2.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	Yes

Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
These changes address the issues with undefined terms and broadens the scope appropriately.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	

If the SDT intends to exclude IRA requirements for EACMS or PACS, we suggest the SDT should clarify Intermediate Systems are not required for EACMS and PACS only if the EACMS and PACS are located outside ESP. We understand that the SDT didn't use the defined term IRA in R3.1 and R3.2, but if an EACMS or PACS is inside an ESP and the vendor remote access meets the IRA definition, does SDT allow a vendor IRA to the EACMS or PACS inside an ESP without compliance with IRA requirements of CIP-005 R2?

Likes 0	
Dislikes 0	

Response
Thank you for your comment. It is not within the scope of the 2019-03 SAR for the SDT to resolve regional interpretation inconsistencies regarding dual classification of EACMS and/or PACS installed inside an ESP and the varied implications on Intermediate System need. The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC's Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC's Compliance & Enforcement team, who can assess and unify audit interpretation.

Janet OBrien - WEC Energy Group, Inc. - 5

Answer	Yes
Document Name	

Comment

Agree with comments submitted separately by Tom Breene of WEC

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see response to WECC.

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the removal of the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments on #1. Texas RE also suggests that defining "system-to-system" could add clarification.	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to question 1. "System-to-system" is already part of the approved language of the standard and this drafting team did not make modifications to that terminology.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

See EEI's comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC appreciates the SDT's proposal, but would offer that references to vendor-initiated remote access should be consistent throughout the body of the supply chain standards. In its review, GSOC identified the following different terms that appeared to be used either interchangeably or with the same or similar objectives:

- In CIP-005, GSOC identified the terms "active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)" in requirement R2.4; "active vendor remote access (including Interactive Remote Access and system-to-system remote access)" in requirement R2.5; and "authenticated vendor-initiated remote connections" in requirements R3.1 and 3.2.
- In CIP-013, GSOC identified the term "vendor-initiated remote access" in requirement R1.2.6.

All of these terms appear to have the same connotation and objective. Yet they are all slightly different in more ways than just reserving technical aspects for the more technical standards.

Utilization of different terms could lead to the interpretation of different scopes or objectives, which would result in confusion, ambiguity, and subjectivity in both implementation and compliance enforcement. Conversely, utilization of the same terms in multiple requirements makes the definition, scope, and objective clearer and simplier. It also makes implementation more straightforward and easier to audit.

For these reasons, GSOC suggests that the SDT consider defining vendor-initiated remote access and, then, utilize the defined term throughout the body of supply chain reliability standards to eliminate the potential for confusion regarding these undefined terms. To facilitate the SDT’s review and potential adoption of this suggestion, GSOC proposes the following definition of vendor-initiated remote access:

User-initiated access by a Vendor employing a remote access client or other remote access technology using a routable protocol and is inclusive of Interactive Remote Access and system-to-system communications. Vendor is defined as those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services, but is not inclusive of other NERC registered entities providing reliability services.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. CIP-005-7 Requirements R3.1 and 3.2 include very specific prescriptive language for “authenticated vendor-initiated remote connections.” However, CIP-013-2 requires the entity to develop a plan to address vendor risk, and therefore the phrase “vendor-initiated remote access” included in requirement R1.2.6 does not need to be as specific or prescriptive, and each entity will determine which vendors are in scope. Vendor is not a defined term, however as written by the original Project 2016-03 SDT and included in the CIP-013-2 Technical Rationale “A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.”

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

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees with the removal of the references to Interactive Remote Access (IRA).

Likes 0	
Dislikes 0	

Response

Response Thank you for your comment.	
Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with comments submitted separately by Tom Breene of WEC	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to WECC.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
The phrase “coordinating controls” in Part 1.2.6 is not defined and should be clarified what it means explicitly.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. When considering a vendor, part of the entity process should be to gain an understanding of how the vendor communicates breaches or vulnerabilities, and then determine what risk the vendor's approach poses. Entities might have established their own standards and expectations for how quickly they expect to be notified of such things and as a part their plan may incorporate certain expectations or legal obligations into the procurement terms with the vendor. These controls in CIP-013 are intended to provide a minimum set of upfront considerations the entity should consider when assessing risk prior to procurement. The operationalization of these controls occurs after the CIP-013 planning requirements are already met. As written by the original Project 2016-03 drafting team, each entity has the flexibility to develop their own risk-based plan to address vendor risk.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	

ISO-NE supports the removal of the references to IRA and the undefined term system-to-system for CIP-013-2. To avoid confusion, ISO-NE recommends that SDT ensures the CIP-013-2 R1.2.6 language and vendor terms remain consistent with the CIP-005 and CIP-010 supply chain requirements.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. CIP-005-7 Requirements R3.1 and 3.2 include very specific prescriptive language for "authenticated vendor-initiated remote connections." However, CIP-013-2 requires the entity to develop a plan to address vendor risk, and therefore the phrase "vendor-initiated remote access" included in requirement R1.2.6 does not need to be as specific or prescriptive, and each entity will determine which vendors are in scope.

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

Answer	Yes
Document Name	

Comment

PG&E believes this modification aligns CIP-013 Requirement P1.2.6 with the modifications made in CIP-005 and removes operational requirements from the CIP-013 plan.

Likes 0	
Dislikes 0	

Response

Thank you for your comment.

David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

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

Answer	Yes
Document Name	

Comment

The SDT should ensure industry understands that CIP-013 Parts R1.2.5 and R1.2.6 are included as security controls required from the relationship of entities and vendors as part of an entities CIP-013 Supply Chain Cyber Security plan – i.e., when establishing a new supply chain vendor relationship with a vendor or enhancing the existing supply chain cyber security relationships. In general, the actions and outputs of a Supply Chain (and CIP-013) program occur before an entity onboards or maintains a system.

The phrase “coordinating controls” is not defined nor well understood in CIP-013

Likes 0	
Dislikes 0	

Response

Thank you for your comments. These CIP-013 requirements are not operational requirements. Those are items to have in your procurement plan and things to consider when doing business with vendors, and then they have “like” parts in the operational standards where day to day execution occurs. These are complimentary requirements with complimentary objectives, and not duplicative nor competing activities with CIP-005-7 R2-R3 and CIP-010-3 R1.6.

When considering a vendor, part of the entity process should be to gain an understanding of how the vendor communicates breaches or vulnerabilities, and then determine what risk the vendor’s approach poses. Entities might have established their own standards and expectations for how quickly they expect to be notified of such things and as a part their plan may incorporate certain expectations or legal obligations into the procurement terms with the vendor. These controls in CIP-013 are intended to provide a minimum set of upfront considerations the entity should consider when assessing risk prior to procurement. The operationalization of these controls occurs after the CIP-013 planning requirements are already met. As written by the original Project 2016-03 drafting team, each entity has the flexibility to develop their own risk-based plan to address vendor risk.

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
The IRC SRC supports the removal of references to IRA and the undefined term, "system to system" from CIP-013-2, requirement R1.2.6. In addition, we agree with the addition of EACMS and PACS to meet what was directed in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report.	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments.	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments.	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree that CIP-013 should remain the Plan while CIP-005 and CIP-010 are technical.	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments.	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
The CAISO supports the ISO/RTO Council Standards Review Committee comments below. The IRC SRC supports the removal of references to IRA and the undefined term, “system to system” from CIP-013-2, requirement R1.2.6. In addition, we agree with the addition of EACMS and PACS to meet what was directed in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report.	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments.	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
please reference Marty Hostler, Northern California Power Agency, comments	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments. Please see response to Northern California Power Agency.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI's comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE notes that the Standard Drafting Team (SDT) removed references to remote access and system-to-system communications from CIP-013-2 R1.2.6 and elected instead to define the term “remote access” in that proposed requirement as included “vendor-initiated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated [Interactive Remote Access (IRA)] and system to system access to BCS and PCAs” in the Technical Rationale document. Texas RE suggests that the SDT instead retain the general requirement that Requirement 1.2.6 apply to system-to-system remote access directly within the requirement	

language. Texas RE further suggests that the SDT could address concerns regarding the requirement that EACMS and PACS themselves have intermediate systems by adding language to Requirement R1.2.6 that excludes Intermediate Systems for EACMS and PACS in the applicability section. Alternatively, the SDT could revise the definition of Interactive Remote Access to clarify this point, obviating the need for the proposed changes to CIP-013-2 R1.2.6.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. CIP-005-7 Requirements R3.1 and 3.2 include very specific prescriptive language for "authenticated vendor-initiated remote connections." However, CIP-013-2 requires the entity to develop a plan to address vendor risk, and therefore the phrase "vendor-initiated remote access" included in requirement R1.2.6 does not need to be as specific or prescriptive, and each entity will determine which vendors are in scope. The SDT decided not to change definition of IRA or any NERC defined terms since that change would impact other existing Standards and that is beyond the scope of this SDT's SAR. In addition, Project 2016-02 is currently reviewing this definition and this comment will be passed to that team for consideration.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. 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.

SDT Response Below:

Thank you for your comments. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.

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

Answer	No
Document Name	

Comment

Unfortunately, there is a continual misplacement and shift of requirements (Parts) related to their given security objectives within the CIP framework. NERC is chartered with the edict to map CIP to NIST and the SDT should keep this in mind when developing standards.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the response at the beginning of question 4.

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

Answer	No
Document Name	
Comment	
PG&E cannot agree the modifications are cost effective since the work to complete the implementation of the CIP-013-1 set of Standards is just being completed and full testing has not been completed to determine the cost of that work. As noted in the PG&E input on the first Comment & Ballot for these modifications, PG&E would have preferred to have an “Unknown” option to select.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see the response at the beginning of question 4.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Do not agree. Tri-State contends that the edits should have been risk-based and only applicable to the control portions of PACS and EACMS, and not also the monitoring portions of those systems. Additionally, time and resources would be saved if the SDT would include language that clarifies that entity-initiated remote access and entity-initiated vendor remote access are not prohibited by CIP standards.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EACMS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Although ISO-NE acknowledges the importance of establishing Supply Chain requirements associated with EACMS and PACS, ISO-NE respectfully believes that it cannot clearly determine if the modified requirements would meet the FERC directives in a cost effective manner because the current CIP-005-6, CIP-010-3 and CIP-013-1 standards have yet to become effective. It is difficult to determine cost-effectiveness when the approach is to build on requirements that the Industry has had limited experience with and limited opportunities for lessons learned or to mature processes and controls.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see the response at the beginning of question 4.	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	No

Document Name

Comment

“vendor-initiate remote access” only seems to apply to R3 of CIP-005-7, so the summary above does not accurately reflect the changes to R2 of CIP-005-7. “Vendor Initiated” should be included in CIP-007 R2.4 and 2.5. Leaving non-vendor initiated remote access in R2.4 and R2.5 is purely administrative in nature. SMUD has implemented this requirement as it is currently written and have found it to be both operationally inefficient and lacking value from a security standpoint.

For R3, this question cannot be answered because it is unclear what constitutes an authenticated vendor-initiated remote connection.

Likes 0

Dislikes 0

Response

Thank you for your comment. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.

The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

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

Answer	No
Document Name	

Comment

To minimize churn among standard versions and better identify the scope, Reclamation recommends the SDT take additional time to coordinate the modifications in CIP-005-7, CIP-010-4, and CIP-013-2 with other existing drafting teams for related standards; specifically, Projects 2016-02, 2020-03, and 2020-04. This will help minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. NERC should foster a standards development environment that will allow entities to fully implement technical compliance with current standards before moving to subsequent versions. This will provide entities economic relief by better aligning the standards for overall improved reliability and by reducing the chances that standards will conflict with one another.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the response at the beginning of question 4.

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

Answer	No
Document Name	

Comment

BC Hydro recommends changing the applicability around PACS to be associated with Medium Impact BCS with ERC instead of just Medium Impact BCS to avoid confusion. The modifications under CIP-010-4 R1.6 to include PACS associated with Medium Impact BES Cyber Systems is otherwise out of alignment in regards to the application of PACS under the CIP standards. The CIP standards under CIP-006-6 require the application of PACS in environments associated with High Impact BES Cyber Systems, Medium Impact BES Cyber Systems with External Routable Connectivity, and associated EACMS and PCAs but do not require this for Medium Impact BES Cyber Systems *without* ERC. By expanding the requirement and application of PACS to Medium Impact BES Cyber Systems without any qualifier per CIP-010-4 R1.6, it is not clear whether this is implied to bring into scope similar or identical cyber assets to PACS that may be used by entities to restrict and/or monitor access to Medium Impact without ERC BES Cyber Systems but which would not meet the definition of PACS (even though the application of these are not required by the standards).

Likes 0	
Dislikes 0	

Response
Thank you for your comment. PACS are not currently required for medium impact BES Cyber Systems without External Routable Connectivity. Furthermore, all requirements in CIP-010-4 are subject to the text in the "Applicable Systems" at the beginning of the standard which states "Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity."

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

Answer	No
Document Name	

Comment

The basic capability of detecting (which is a better term than determine) remote session activity is the relevant security control. Whether that activity is initiated by a vendor, partner, customer, or an employee is irrelevant to the technical capability. Scoping the requirement narrowly does not provide significant cost savings and still allows for poor security. BPA does not agree with feedback that monitoring for remote sessions by employees could be a union issue. There is a difference between monitoring for external sessions vs monitoring employee activity within a session and this requirement does not go that far. Insider threat remains the number one threat to critical infrastructure and the ability to actively detect and terminate a session regardless of who originates it is a key cyber security control.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. FERC Order 850 and the drafting team SAR, directed the SDT to modify the standard to specifically deal with vendors, any additions to the standard language would be considered outside the scope of the SAR.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST recommends modifying proposed changes to CIP-005, as per our response to Question 1.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response is question 1.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
please reference Marty Hostler, Northern California Power Agency, comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to Northern California Power Agency.	
Andrea Barclay - Georgia System Operations Corporation - 4	

Answer	Yes
Document Name	
Comment	
GSOC agrees that the SDT has worked to fine tune requirements to ensure security and cost-effectiveness. However, GSOC remains concerned about the scope of EACMSs to which the requirements are applicable and how the current scope increases the overall cost and burden on registered entities. For these reasons, GSOC recommends that the SDT work on additional fine-tuning of the overall scope of applicability as related to EACMSs. Additionally, GSOC notes that the multiple requirements, “interchangeable” terms, and potential for confusion and ambiguity detract from the potential cost-effectiveness of these standards. The elimination of multiple, “interchangeable” terms through the use of definitions and defined terms along with streamlined requirements will help to further fine-tune the scope and security obligations set forth within these standards. They will also facilitate consistent, effective compliance auditing, making these reliability standards more cost-effective across the ERO Enterprise.	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EACMS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	

Cost effective is vague. Please provide a cost/benefit justification for any posposed changes.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see the response at the beginning of question 4.	
Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with comments submitted separately by Tom Breene of WEC	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to WECC.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We recommend defining the term ‘Vendor Initiated Remote Access’, and define who is considered a vendor.	

Likes 0	
Dislikes 0	
Response Thank you for your response. Vendor is not a defined term, however as written by the original Project 2016-03 SDT and included in the CIP-013-2 Technical Rationale “The term vendor(s) as used in the standard is limited to those persons, companies, or otherorganizations with whom the Responsible Entity, or its affiliates, contract with to supply BESCyber Systems and related services. It does not include other NERC registered entities providingreliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant toNERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers ormanufacturers of information systems, system components, or information system services; (ii)product resellers; or (iii) system integrators.”	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC

Answer	
Document Name	

Comment

The CAISO supports the ISO/RTO Council Standards Review Committee comments below.

While the IRC SRC acknowledges that EACMS and PACS are important to protect and believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory compliance has the potential to increase the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. NERC and the industry should continue to monitor and evaluate cost versus security benefits.

In that regard, the IRC SRC proposes that after CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years, NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the response at the beginning of question 4.

Becky Webb - Exelon - 6

Answer	
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

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

Likes 0

Dislikes 0

Response

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

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks

Answer

Document Name

Comment

While the IRC SRC acknowledges that EACMS and PACS are important to protect and believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory compliance has the potential to increase the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. NERC and the industry should continue to monitor and evaluate cost versus security benefits.

In that regard, the IRC SRC proposes that after CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years, NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see the response at the beginning of question 4.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	
Comment	
No comment on cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	

Thank you for your response.

David Jendras - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

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

Neil Shockey - Edison International - Southern California Edison Company - 5

Answer	
Document Name	

Comment

See EEI's comments

Likes 0	
Dislikes 0	

Response

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

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy sees potential schedule and cost risks in implementing yet to be defined tools.	
Likes 0	
Dislikes 0	
Response Thank you for your response.	

5. Provide any additional comments for the standard drafting team to consider, if desired.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	

Answer

Document Name

Comment

The wording in CIP-013 R1.2.6 should match the wording in CIP-005-7 R3 P3.2, to wit: “authenticated vendor-initiated remote connections”

Likes 0

Dislikes 0

Response

Thank you for your comment. CIP-005-7 Requirements R3.1 and 3.2 include very specific prescriptive language for “authenticated vendor-initiated remote connections.” However, CIP-013-2 requires the entity to develop a plan to address vendor risk, and therefore the phrase “vendor-initiated remote access” included in requirement R1.2.6 does not need to be as specific or prescriptive, and each entity will determine which vendors are in scope.

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

Answer

Document Name

Comment

Thank you for the opportunity to comment.

Likes 0

Dislikes 0

Response

Thank you for your response.

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

Answer	
Document Name	

Comment

The SDT uses the term “sessions” in CIP-005-7 R2 but in CIP-005-7 R3, it proposes replacing the term “session” with “connection.” Since there is no definition of “connection” in the *Glossary of Terms Used in NERC Reliability Standards* or in the NIST online glossary, BPA believes the term “connection” is ambiguous and should not be used within the standard.

Proposed change to CIP-005-7 R3.1:

Have one or more method(s) for detecting remote access sessions.

Proposed change to CIP-005-7 R3.2:

Have one or more method(s) for terminating remote access sessions.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

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

Answer	
Document Name	
Comment	
Further clarity should be provided regarding the definition of "vendor" in relation to staff augmentation consultants/contractors who may performing system integration work or supporting/managing the operation of BES Cyber Assets via remote access. NERC had during CIP-013-1 standard development responses to industry, indicated that it does not consider staff augmentation contractors/consultants who are treated similar to employees to be considered vendors. However, WECC is communicating a different approach in compliance outreach sessions and are expecting entities to identify staff augmentation contractors/consultants to be considered as vendors due to risks they could pose. This should be clarified within the standards to either allow entities the flexibility to define who vendors are to them ***or*** to have the standard drafting team define this clearly through a proposed Glossary defined term or within the standard language itself as the current definition within the standard is open to interpretation between enforcement entities and create undue compliance burden.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT has provided guidance in Technical Rationale which states "The term vendor(s) as used in the standard is limited to those persons, companies, or otherorganizations with whom the Responsible Entity, or its affiliates, contract with to supply BESCyber Systems and related services. It does not include other NERC registered entities providingreliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant toNERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers ormanufacturers of information systems, system components, or information system services; (ii)product resellers; or (iii) system integrators." The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC's Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC's Compliance & Enforcement team, who can assess and unify audit interpretation.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	

Comment

In regards to CIP-010-4 Requirement 1 Part 1.6, PCAs should also be included in the Applicable Systems. When BES Cyber Systems and PCAs are located within the same ESP and software is validated and verified for the BCS but not the PCAs, a mixed-trust security environment is created within an ESP. By not including PACs in the Applicable Systems, it poses additional unnecessary risk to the security of the BES.

Likes 0

Dislikes 0

Response

Thank you for your comment. The NERC Supply Chain report did not recommend including PCAs at this time.

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer

Document Name

Comment

The language is very clear in this version.

Likes 0

Dislikes 0

Response

Thank you for your comment.

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

Answer

Document Name

Comment	
Reclamation recommends a 24-month implementation plan to allow entities flexibility to determine the appropriate implementation actions.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Based on industry comment, the SDT determined that an 18 month implementation plan was appropriate.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	
Comment	
PG&E has no additional input regarding this Comment & Ballot.	
Likes 0	
Dislikes 0	
Response Thank you for your response.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	

MEC supports EEI comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI's comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	

Regarding the Implementation Guidance for CIP-005-7, we provide the following four (4) comments:

(1) Page 3, 2nd paragraph - Suggest adding 'within the Electronic Security Perimeter' as EACMS can reside within the ESP and this appears to be the context of these EACMS.

(2) 'However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS,'

Change to "However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS within the Electronic Security Perimeter,[…]"

(3) Page 5, 2b 'Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and architecture'

Suggest different wording than architecture. Perhaps network topology?

(4) Page 7 - While this section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is from the CIP-005-6 standard, consider detailing the first use of EAP as it isn't used anywhere prior in the IG. Change 'Responsible Entities should know what traffic needs to cross an EAP' to "Responsible Entities should know what traffic needs to cross an Electronic Access Point (EAP)..."

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT has taken these comments into consideration and modified the Implementation Guidance based on comments 1-3. The section of the GTB that is cut and paste from CIP-005-6 will remain intact in its historical version.

Jose Avendano Mora - Edison International - Southern California Edison Company - 1

Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	

Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	
Document Name	
Comment	
The IRC SRC requests the SDT create individual ballots for each standard included in this project. This would provide flexibility to the industry to support certain aspects of this project while expressing concerns over other aspects.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The standards were balloted together as they are collectively referred to as the supply chain risk management Reliability Standards per FERC Order 850. The SDT choose to ballot all the standards together to ensure they all passed industry approval to meet the deadline in FERC Order 850.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	

Document Name	
Comment	
We appreciate the SDT efforts.	
Likes 0	
Dislikes 0	
Response Thank you for your response.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	

Comment

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

Likes 0

Dislikes 0

Response

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

Becky Webb - Exelon - 6

Answer

Document Name

Comment

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

Likes 0

Dislikes 0

Response

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

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer

Document Name

Comment	
Westar Energy and Kansas City Power & Light, the Evergy companies, support and incorporate by reference the Edison Electric Institute's response to Question 5.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	
Comment	

In the Technical Rationale for Reliability Standard CIP-013-2 document (page 11), “Requirement R2” should read “Requirement R3”. The text indicates “The proposed requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P.46) “. R2 requires the responsible entity to implement its supply chain cyber security risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Technical Rational for CIP-013-2 Page 11 is the historical section preserving the CIP-013-1 Technical Rationale. This has been corrected in the main body of the document.

Monika Montez - California ISO - 2 - WECC

Answer	
Document Name	

Comment

The CAISO supports the ISO/RTO Council Standards Review Committee comments below.

The IRC SRC requests the SDT create individual ballots for each standard included in this project. This would provide flexibility to the industry to support certain aspects of this project while expressing concerns over other aspects.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The standards were balloted together as they are collectively referred to as the supply chain risk management Reliability Standards per FERC Order 850. The SDT choose to ballot all the standards together to ensure they all passed industry approval to meet the deadline in FERC Order 850.

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Comments from EEI

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   □ No

   Comments: While EEI supports the changes made by the SDT, which addressed prior EEI member comments related to CIP-005-7 Requirement R2 Parts 2.4 and 2.5, we recommend the SDT revise “vendor remote access” to “vendor initiated remote access” or explain why all vendor remote access needs to be evaluated for Parts 2.4 and 2.5.

   EEI supports the current proposed draft language for Requirement R3.

   Response: Thank you for your comments. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry’s concerns about recursive requirements (‘hall of mirrors’). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   □ No

   Comments: EEI supports the changes made by the SDT to address prior EEI member comments related to the “hall of mirrors” issue.

Response: Thank you for your comment.

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   □ No

   Comments:

   Response:

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. 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.

   □ Yes

   □ No

   Comments: EEI has no comment on the cost effectiveness of the proposed changes.

   Response: Thank you for your response.

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

   Comments: EEI previously provided comments that CIP-005-7 did not provide sufficient clarity regarding contractors who are essential to the reliable operation of the BES. Specifically, the Reliability Standard did not provide a mechanism that exempted contractors who provided essential contract services. Although CIP-005-7 does not explicitly provide a defined process for exempting these contractors, the draft Implementation guidance makes it clear that these types of contractors are to be handled in a manner similar to the staff of a registered entity.

   Response: Thank you for your comment.

End of Report