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 2)
Comment Period Start Date:	5/7/2020
Comment Period End Date:	6/22/2020
Associated Ballot:	2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 AB 2 ST

There were 75 sets of responses, including comments from approximately 183 different people from approximately 124 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.

Questions

1. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. Do you agree that this proposal makes it clearer that Intermediate Systems are not required? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT is proposing language in CIP-005-7 in the newly formed R3 to clarify remote session conditions. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. The SDT is proposing removing the exception language in CIP-010-4 "Applicable Systems" for PACS which stated "except as provided in Requirement R1, Part 1.6." This reverts the language in this section back to what is in CIP-010-3. Do you agree with this proposed modification? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. To address comments the SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 to clarify that all types of vendor-initiated remote access needs to be considered. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendations and if appropriate, technical or procedural justification.

5. The SDT is proposing an increase from 12 to 18 month implementation plan in response to industry comment. Do you agree this strikes a balance between appropriate risk mitigation and giving the industry time to implement changes?

6. 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. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

7. 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
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	Bobbi Welch	MISO	2	RF
					Ali Miremadi	CAISO	2	WECC
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
Santee Cooper	Chris Wagner	1		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Andy Crooks	SaskPower Corporation	1	MRO
					Bryan Sherrow	Kansas City Board of Public Utilities	1	MRO
					Bobbi Welch	Omaha Public Power District	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Bobbi Welch	Midcontinent ISO	2	MRO
					Douglas Webb	Kansas City Power & Light	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO
					James Williams	Southwest Power Pool, Inc.	2	MRO
					Jamie Monette	Minnesota Power / ALLETE	1	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Sing Tay	Oklahoma Gas & Electric	1,3,5,6	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Troy Brumfield	American Transmission Company	1	MRO
NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk	3		NIPSCO	Joe O'Brien	NiSource - Northern Indiana Public Service Co.	6	RF
					Kathryn Tackett	NiSource - Northern Indiana Public Service Co.	5	RF
					Steve Toosevich	NiSource - Northern Indiana Public Service Co.	1	RF
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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Public Utility District No. 1 of Chelan County	Ginette Lacasse	1	WECC	PUD #1 Chelan	Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
					Ginette Lacasse	public Utility Distric No 1 of Chelan	1	WECC
Snohomish County PUD No. 1	Holly Chaney	3		SNPD Voting Members	John Martinsen	Public Utility District No. 1 of Snohomish County	4	WECC
					John Liang	Snohomish County PUD No. 1	6	WECC
					Sam Nietfeld	Public Utility District No. 1 of Snohomish County	5	WECC
					Alyssia Rhoads	Public Utility District No. 1 of	1	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Snohomish County		
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jim Davis	East Kentucky Power Cooperative	1,3	SERC
					Scott Brame	North Carolina EMC	3,4,5	SERC
					Ryan Strom	Buckeye Power, Inc.	5	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Meredith Dempsey	Brazos Electric Power	1,5	Texas RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Cooperative, Inc.		
					Carl Behnke	Southern Maryland Electric Cooperative	3	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
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF

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	4	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
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
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
					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
					John Pearson	ISO-NE	2	NPCC
					David Kiguel	Independent	7	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					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
					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	3	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Edison Co. of New York		
					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
					Randy MacDonald	NB Power Corporation	2	NPCC
					Jim Grant	NY-ISO	2	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					John Hasting	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	6	SPP RE	OKGE	Sing Tay	OGE Energy - Oklahoma	6	MRO
					Terri Pyle	OGE Energy - Oklahoma Gas and Electric Co.	1	MRO
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Lower Colorado River Authority	Teresa Cantwell	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. Do you agree that this proposal makes it clearer that Intermediate Systems are not required? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Erick Barrios - New York Power Authority - 6	
Answer	No
Document Name	
Comment	
Vendor remote access is part of remote access. It is not clear why these are separated. Additional confusion caused by another SDT will modify the "interactive remote access" definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project. More confusion from the "hall of mirrors" – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments, which were identical to those submitted by the NPPC RSC comments. Please see the SDT's response to RSC NPPC's comments.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
R2 states "For all Interactive Remote Access, utilize an Intermediate System". However, by creating a new requirement specifically for vendor access there could be confusion that the access is "vendor" related access and R2 is not applicable. Based on the wording of this Question as context, it appears that it's the intent of the SDT to remove intermediate systems for vendor initiated IRA. Thus explicitly allowing direct vendor access to assets in the ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. CIP-005-7 R2 Part 2.1 is also silent to the initiator of the access, and therefore IRA is one type of vendor remote access in the context of the BCS and its associated PCAs, and pursuant to CIP-005-7 R2 Part 2.1 the use of an Intermediate System is required. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT intention is to be clear that an Intermediate System is not required for remote access to EACMS and PACS specifically. The changes made to CIP-005-7 R3 to apply only to EACMS and PACS should clarify the concern.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No

Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	
Response	

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State recommends that CIP-005-7 R3 plane definitions be expanded, as they are brief and there is no further explanation of the planes in the Implementation Guidance or Technical Rationale. Suggest definitions similar to Cisco examples below:

1) Management plane of a system is that element that configures, monitors, and provides management, monitoring and configuration services to, all layers of the network stack and other parts of the system. Examples include protocols such as Telnet, Secure Shell (SSH), TFTP, SNMP, FTP, NTP, and other protocols used to manage the device and/or network. 2) Data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic. End-station, user-generated packets that are always forwarded by network devices to other end-station devices. From the perspective of the network device, data plane packets always have a transit destination IP address and can be handled by normal, destination IP address-based forwarding processes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT will consider your suggested language for the Implementation Guidance or Technical Rationale.	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
The measures include as examples the usage of an EAP or Intermediate System to disable access. By the very nature of the devices, PACS and EACMS are outside of network boundary inclusion for CIP. To now require that termination of vendor access for EACMS and PACS by definition and available technology have required that controls be placed on these devices that contain assets outside of NERC CIP scope. EACMS and PACS should not be included in scope for Supply Chain management until or unless they are required to be placed behind a Firewall and required access via an Intermediate Server. The not do so leaves entities exposed to a wide interpretation during audit on what is an “acceptable” method for identification and termination of vendor access.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. To require an Intermediate System for access into the EACMS would be recursive. The SDT was mindful not to create a 'hall of mirrors'. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. LaGrange has been added to CIP-005-7 R3 Part 3.1 to clarify what is required. That having been said, these requirements do not preclude and entity from going above and beyond the minimums of the Standards to implement a defense in depth approach with additional layers of security.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments The changes which move Vendor Remote Access remote access from Parts 2.4 and 2.5 to Parts 3.1 and 3.2 better clarify the requirements for entities, however adding EACMS to the scope of the standard requires an Intermediate System to access an EACMS; and because an Intermediate System is already defined as an EACMS (because it provides electronic access), and hence the change requires an entity to deploy a separate Intermediate (EACMS) to access the Intermediate System that provides access to the BCS. The entity must implement another upstream control beyond that EACMS in order to disable the access "to" it, thereby creating another upstream device that qualifies as an EACMS by definition. Recommend language to clarify the term access. This could be "authenticated access, access session, etc..." so it is clear that "a knock on the front door" of the EACMS that authenticates the system/user is NOT considered "access" (or in this case, by extension, "vendor remote access") to an EACMS. This would preclude auditors from interpreting a "knock at the front door of the EACMS that is later denied within the EACMS" as "access to" an EACMS.

Additionally, Requirement R3 Part 3.2 is a "how" in disguise instead of an objective "what". Another potential solution to consider could be the following: Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability to for a vendor to establish and use remote access". If this were the language, then "terminating established vendor remote access sessions" is one way "how" an entity could meet this objective (although it highlights the gap in the existing draft that terminating established sessions alone may not preclude the re-establishment of another session). This language could also resolve the hall of mirrors because now the entity can define the revocation point that precludes authentication and subsequent use within the layers of EACMS controls, and the "knock at the front door" to the EACMS is no longer "access". Another consideration is to revise CIP-002 to allow entities to define only those systems they use as Intermediate Systems and/or Remote Access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered MRO NSRF's suggestion to add clarifying language to the term "access", to help assure the perceived 'hall of mirrors' issue is resolved. The use of an Intermediate System for EACMS is not required. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1. The SDT added clarifying language to CIP-005-7 R3 Part 3.1 to remove concerns with "knock at the front door" issues. The SDT has considered MRO NSRF's comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap from the use of the word 'terminate', and to add the necessary flexibility for an entity to determine how to meet the security objective. Modifications to CIP-002 are out of scope of the 2019-03 SAR.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	

Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) supports the comments as submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy does not agree that the modifications made to the second draft of CIP-005-7, Requirement R3 clarify that Intermediate Systems are not required. This modification conflicts with Requirement R2, subpart 2.1, which requires the use of Intermediate Systems	

for all interactive remote access sessions regardless of the source of initiation. In addition, the definition of EACMS currently includes Intermediate Systems. Based on these reasons, Intermediate Systems cannot be excluded. Moreover, Requirement R3 makes EACMS applicable to this requirement. Additionally, Dominion Energy continues to opine that EACMS should be excluded from the applicability section of Requirement R2, subpart 2.5. Moving this requirement, along with the minor modifications included in this draft, has not solved the issues identified in our comments to the earlier draft of CIP-005-7.

Dominion Energy is also of the opinion that "vendor remote access" includes both Interactive Remote Access (IRA) as well as system-to-system access. Consequently, entities would be required to determine the identity of the source of communications before they can establish a session with the Intermediate System, which is not possible because sSystems must establish a session with the Intermediate System in order to receive user credentials, which are then generally checked with another EACMS (such as a domain controller) in order to determine whether the source is a vendor. At this point, the vendor's system has already had access to the entity's EACMS.

Dominion Energy is of the opinion that the SDT should consider removing EACMS from the scope of CIP-005 Requirement R3. We understand that the security objective for this requirement is to determine and disable vendor remote access sessions to BES Cyber Systems by using EACMS. If this is incorrect, we ask the SDT to more clearly described the objective.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT must include EACMS in CIP-005-7 to meet FERC directives. In Order No. 850 the "supply chain risk management Reliability Standards" is a term that collectively refers to CIP-013-1, CIP-005-6, and CIP-010-3. Therefore, any directives which pertain to the supply chain risk management Reliability Standards pertain to the entire set of above listed Standards. Specifically, paragraph 1 describes the term at the outset of the Order No. 850:

"Pursuant to section 215(d)(2) of the Federal Power Act (FPA), the Commission approves supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)."

Paragraph 5 of Order No. 850 is the first time instance of the directive:

"To address this gap, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…"	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends revising the language of CIP-005-7 R2 Part 2.1 to account for the addition of R3. It is not clear if Part 2.1 carries over and applies to R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intends for CIP-005-7 R2 Part 2.1 to apply for high and medium impact BES Cyber Systems and their associated PCAs, as well as for medium impact BES Cyber Systems with external routable connectivity and their associated BCAs as it relates to vendor remote access. The SDT does not intend for CIP-005-7 R2 Part 2.1 to apply to vendor remote access for EACMS nor PACS. The use of an Intermediate System for EACMS and PACS is not required in the current CIP-005-6 Standard regardless of whether the access is from a vendor or other remote source. Increasing the scope of Intermediate System use to EACMS and PACS is not in scope of the 2019-03 SAR nor is it a directive in the FERC order, therefor, the SDT has made modifications to assure the scope of Intermediate System use is not increased.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	

Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see the response to Snohomish PUD.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Moving the language to the new R3 requirement does not make it clearer that Intermediate systems are not required for R3. If this is the SDT's intent, then it should directly state it in the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA notes that the proposed language still cites applicability to EACMS; Intermediate Systems are included in the definition of EACMS so the language still appears to include a requirement to determine active sessions to an Intermediate System, even if the remote session does not continue on the provide access to an asset in the ESP. In addition, not all EACMS are the same; this term has become too inclusive of many different types of technology to apply requirements.

BPA believes the crux of the problem, as demonstrated by previous comments and unofficial ballot responses by multiple entities, is this: The EACMS definition is concurrently being modified by the 2016-02 project and keeping the current definition inclusive of logging and monitoring systems is problematic for the same reasons in both drafting efforts. The level of threat to and risk from a system that 'controls access' vs a system that provides a support function by 'logging or monitoring access and access attempts' is different. Logging and monitoring systems benefit from global oversight and gathering logs from the entire enterprise. Access granting systems benefit from specificity and narrow focus on the asset they are protecting. The CIP standards **must not** discourage or penalize efforts on the part of an entity to modernize their SIEM and threat analysis capability. Adding compliance burden to their enterprise logging and monitoring systems is such a discouragement.

From a standards standpoint, this is not a common approach to address access control and access monitoring, as they are mutually exclusive. Even FISMA breaks them apart as control families as Access Control (AC) and Audit and Accountability (AU) to address access control and access monitoring respectively, as an example.

An example of more precise language (and BPA suggests this for inclusion in Guidelines and Technical Basis) might be:

R3.1 Have one or more methods for DETECTING active sessions (including both system-to-system and Interactive Remote Access, regardless of the identity of the person initiating the session) that traverse an EAP to logically access any applicable cyber asset in the ESP or ESZ.

R3.2 Have one or more method(s) to TERMINATE active sessions as referred to in R3.1

R3.3 Have one or more method(s) to DISABLE INITIATION OF NEW remote access sessions as referred to in R3.1.

Please note the terminology and conceptual change to a 3 part requirement: "Detect/Terminate/Disable". The word "Determine" is unusual usage and not aligned with typical cyber security terminology. The reason for a separate requirement in our proposed R3.3 is simple; terminating existing sessions does not prevent an attacker from spawning new sessions, and it is very easy to automate such requests. The requirement to "disable active vendor remote access" is crippled by the word "active" because it does not clearly express a

need to disable future sessions which are by definition not "active". Combining the two requirements is parsimonious of words to the point of obscuring the objective. Without a means of denying new sessions, whether granularly or globally, an entity could find themselves playing "whack-a-mole" with an adversary and never able to manually keep it with automated requests. An example of granular control might be disabling a specific vendor's remote access account, blocking requests from a specific IP address or range, or changing an authentication token or password for a particular user account's remote access. This could be an absolute block or a suspension on new sessions for a timed period. For a global option, examples include simply denying all remote access attempts via change to a global VPN policy, firewall rule, etc. This is the proverbial "take a fire axe to the Internet connection" option.

The measures column for CIP-005=07 R3.1 includes *"Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access."* While this may be an effective measure for requiring authorization for a remote session, this is not an effective measure for determining an active session, sans a requirement to periodically/automatically terminate active sessions.

The measures column for R3.2 better captures the concept that the remote access to the Intermediate System or other EACMS is not the issue; simply getting a login prompt to a cyber-asset outside the ESP is low risk. Another means of clarifying the risk around Intermediate Systems might be to add Intermediate System to the applicability column to apply the R3.1 requirement to have a detective control, and leave it out of the R3.2(/R3.3 if adopted) applicability column, not requiring a specific ability to terminate/deny sessions to Intermediate Systems, but rather into the ESP/ESZ.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT agrees that a login prompt on an EACMS does not constitute access. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.

The Electronic Access Control or Monitoring (EACMS) definition is used pervasively within the CIP Standards and it is out of the SDT scope of the 2019-03 SAR to modify NERC Glossary of Terms definitions that impact CIP Standards outside those that are considered the supply chain risk management Reliability Standards; CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). For

this reason, the SDT has not modified the EACMS definition. Additionally, the 2019-03 team has worked with the 2016-02 team to ensure continuity of changes, at this time both teams assert the change of the EACMS definition is outside of each team's respective SARs. The SDT thanks BPA for offering adjusted language and, as requested, is considering those suggestions for the IG or TR (formerly know and GTB). Furthermore, the SDT has considered comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap of reestablished sessions, to assure the spawing of new sessions is addressed, and to add the necessary flexibility for an entity to determine how to meet the security objective.	
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	No
Document Name	
Comment	
Tacoma Power thanks the SDT for considering our previous comments. Unfortunately, moving the language to a new requirement does not clarify the situation. Our concern is that the typical device used to detect a vendor remote access session is the EACMS that the vendor is accessing. Applying this requirement to an EACMS appears to be requiring an EACMS for an EACMS, producing a hall of mirrors. Additionally, the term "active" has been removed from the language, removing this requirement's role in support of the Part 3.2 requirement, since there is no time-bound nature to the current Part 3.1 language. We could have a method to detect after-the-fact vendor-initiated access, which would serve the Part 3.1 requirement language, but not the needs of Part 3.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The word "all" in CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of	

EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT has considered comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap from the removal of the word 'active', and to add the necessary flexibility for an entity to determine how to meet the security objective such that the interests of both Parts 3.1 and 3.2 are served.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
If intent is to specifically denote that intermediate systems are not required or in scope, suggest stating so directly: “Intermediate are not required for R3”.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	No
Document Name	
Comment	
Vendor remote access is part of remote access. It is not clear why these are separated.	

Additional confusion caused by another SDT will modify the "interactive remote access" definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project. More confusion from the "hall of mirrors" – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, which were identical to those submitted by the NPPC RSC comments. Please see the SDT's response to RSC NPPC's comments.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Oncor supports the comments submitted by EEI. In addition, without including the language that "Intermediate Systems are not required", it is left to interpretation by the entity. In CIP-005-6, R2.1 and 2.2, use of an Intermediate System is clearly defined.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for our comment, please see the response to EEI comments.	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see the response to Tacoma Power.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
ATC thanks the SDT for attempting to resolve this concern, and agrees with the approach to separate this requirement out into R3; However, unfortunately the hall of mirrors condition still exists with EACMS in the applicability column due to a broader issue of ambiguity in the word "access". Where getting "to" an EACMS associated with a high or medium impact BES Cyber System is considered "access" (or in this case, by extension, "vendor remote access") the entity must still implement another upstream control beyond that EACMS in order to disable the access "to" it, thereby creating 1) another upstream device that qualifies as an EACMS by definition, 2) a hall of mirrors, and 3) an impossibility of compliance. ATC requests consideration of qualifying language that includes "authenticated access", or something of the like, as the target instead of the ambiguous term "access" so it is clear that "a knock on the front door" of the EACMS that authenticates the system/user is NOT considered "access" (or in this case, by extension, "vendor remote access") to an EACMS. This resolves the hall of mirrors issue and provides necessary specificity to preclude auditors from interpreting a "knock at the front door of the EACMS that is later denied within the EACMS" as "access to" an EACMS.	

Additionally, Requirement R3 Part 3.2 is a "how" in disguise instead of an objective "what". Another potential solution to consider could be the following: Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability for a vendor to establish and use remote access". If this were the language, then "terminating established vendor remote access sessions" is one way "how" an entity could meet this objective (although it highlights the gap in the existing draft that terminating established sessions alone may not preclude the re-establishment of another session). This language could also resolve the hall of mirrors because now the entity can define the revocation point that precludes authentication and subsequent use within the layers of EACMS controls, and the "knock at the front door" to the EACMS is no longer "access".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS is not required. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required. EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. The SDT has considered ATC's comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap from the use of the word 'terminate', and to add the necessary flexibility for an entity to determine how to meet the security objective.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment	
NV Energy supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
The proposed changes dated 05/14/2020 do not provide clarity regarding the applicability of CIP-005 R2, which includes the need for an Intermediate System for **all** Interactive Remote Access Sessions. The requirement language does not distinguish between vendors vs. non-vendors; therefore, Intermediate Systems would be required for vendor Interactive Remote Access sessions. Additionally, the current definition for Interactive Remote Access (IRA) in the NERC Glossary of Terms implies R1 and R2 may still be applicable to the new R3. ISO-NE recommends that the SDT incorporate the new IRA definition proposed by the Virtualization SDT in Project 2016-02 Modifications to CIP Standards into this project. ISO-NE also recommends that the SDT return the language that was moved to the new R3 back to CIP-005 R2.4 and R2.5 in order to maintain continuity with the other CIP-005 R2 remote access requirement parts.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT has elected to keep EACMS and PACS out of Requirement R2 Part 2.1 to prevent confusion of the 'hall of mirrors' and believes the consistency gained by reintroducing EACMS and PACS to Requirement R2 Part 2.1 would not be worth the ambiguity it breeds. For these reasons, SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS or PACS is not required. The Interactive Remote Access (IRA) definition is used pervasively within the CIP Standards and it is out of scope of the 2019-03 SAR to modify NERC Glossary of Terms definitions that impact CIP Standards outside those that are considered the supply chain risk management Reliability Standards; CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). Additionally, the 2016-02 has a specific directive in their SAR to address the NERC V5-TAG issues, for which IRA is one. For these reasons the SDT has not modified the IRA definition.	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to Tacoma Power.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No

Document Name	
Comment	

Southern does not agree that the new R3 makes it clearer that Intermediate Systems are not required. In CIP-005 R2 Part 2.1, Intermediate Systems are required for ALL Interactive Remote Access sessions regardless of who initiates them. If the intent of this question is about clarity that terminating established vendor-initiated remote access sessions *to an Intermediate System* is no longer required, the answer is no. EACMS is in the Applicability column and the definition of EACMS is "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.**" By the definition of EACMS, Intermediate Systems are still included in R3.

The proposed requirement would still require the ability to terminate vendor-initiated remote access sessions to the systems most often used to determine whether the session is vendor-initiated or not. Since the undefined term "vendor remote access" we believe includes both IRA and system-to-system access per the currently approved standard, it appears we would be required to determine the identity of the person BEFORE we allow their system to establish a session with our Intermediate System, which is not possible. The vendor's system must establish a session with the Intermediate System in order to even send the user credentials, which are then checked with usually yet another EACMS (such as a domain controller) in order to determine they are a vendor. At that point, the vendor's system has already had access to our EACMS.

We are also concerned about what "remote" means in context of an EACMS such as an Intermediate System. The definition of Intermediate System states it must NOT be located inside an ESP. The Intermediate System is already remote according to most definitions of remote ('outside the ESP') so what is remote to a remote system?

Southern believes for these reasons that EACMS should either not be in the scope of these particular CIP-005 requirements and the security objective is to be able to determine and disable vendor remote access sessions to BES Cyber Systems *by using EACMS to do so*. If there is some other vendor EACMS access that is intended, it should be precisely described and used within a separate requirement from the main objective of protecting the BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The word "all" in CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.

The SDT agrees that by definition an Intermediate System is an EACMS, and therefore also agree that an Intermediate System is in scope for the proposed protections where that Intermediate System is the target (or endpoint) of the vendor's remote access. This does not suggest that the Intermediate System must be used for vendor remote access to an EACMS. Instead it means that if an entity has outsourced some function for that Intermediate System to a vendor, and that vendor is compromised, the entity must be able to detect the vendor's established connections 'into' the Intermediate system and take action to remove that vendor's ability to retain that connection (or re-initiate subsequent connections). This vendor remote access 'into' the Intermediate System (EACMS) could be human interaction or machine to machine. EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a connection that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a connection that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. The SDT added clarifying language in the Requirement 3, Parts 3.1 and 3.2.

The SDT must include EACMS in CIP-005-7 to meet FERC directives. In Order No. 850 the “supply chain risk management Reliability Standards” is a term that collectively refers to CIP-013-1; CIP-005-6 R2.4 and R2.5; CIP-010-3 R1.6. Therefore, any directives which pertain to the supply chain risk management Reliability Standards pertain to the entire set of above listed Requirements, unless specifically excluded by the directive. Specifically, paragraph 1 describes the term at the outset of the Order No. 850:

“Pursuant to section 215(d)(2) of the Federal Power Act (FPA), the Commission approves supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments).”

Paragraph 5 of Order No. 850 is the first time instance of the directive:

"To address this gap, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" For additional clarity, the focus is not limited to vendor remote access through an EACMS into a BCS. The focus also includes vendor remote access into the EACMS or PACS itself, which could ultimately lead to further unauthorized access to the BCS. Otherwise stated with EACMS as the use case, if an entity allows a vendor's untrusted (or less-trusted) system or personnel to remotely connect machine-to-machine or user-to-machine into the entity's EACMS, and the vendor's system is compromised, then that entity must make sure the vendor's compromised system and personnel are no longer connected remotely into the entity's EACMS. The security objective is remove a vendor's ability to retain or reestablish remote access sessions for each of these discrete Cyber Systems: - high impact BES Cyber Systems; - EACMS associated to high impact BES Cyber Systems; - PACS associated to high impact BES Cyber Systems; - medium impact BES Cyber System with External Routable Connectivity; - EACMS associated to medium impact BES Cyber System with External Routable Connectivity; and - PACS associated to medium impact BES Cyber System with External Routable Connectivity."

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

We do not believe this requirement is clear with respect to Intermediate Systems. For any Interactive Remote Access, an Intermediate System should be required, no matter the source (vendor vs. internal).

Second, the second bullet in the measures for Part 3.1 discusses monitoring remote activity, which is inconsistent and exceeds the requirement to detect remote access sessions.

Third, the third bullet in the measures for Part 3.1 needs to better explain the methodology the SDT is intending to describe.

Lastly, the SDT is making an arbitrary distinction for vendor remote access that is unnecessary. All remote access (vendor or internal) should be similarly treated in terms of detecting and termination. However, as discussed previously, the expectation for monitoring is not part of the identified requirements and should be removed from the measures.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. To require an Intermediate System for access into the EACMS would be recursive. The SDT was mindful not to create a 'hall of mirrors'. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. That having been said, these requirements do not preclude and entity from going above and beyond the minimums of the Standards to implement a defense in depth approach with additional layers of security. The SDT appreciates the security focus that remote access should be treated similarly, however, this is a critical distinction that is necessary, especially in the context of union agreements where an entity could be faced with an impossibility of compliance if required to monitor activity and detection of established union personnel. Additionally, it stands to reason that vendor remote access, as a function of its risk, be treated differently and more rigorously than remote access by the entity. For these reasons, the SDT was mindful to separate out vendor remote access to assure the activity monitoring and session detection components of vendor access are not extended to an entity's employee base.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	

We appreciate the SDT efforts. However, this does seem to create a "hall of mirrors" as pointed put by a number of commenters by requiring an intermediate system for an intermediate system. There should also be allowance for CIP exceptional circumstances in CIP-013.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Vendor remote access is part of remote access. It is not clear why these are separated.

Additional confusion caused by another SDT will modify the “interactive remote access” definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project.

More confusion from the “hall of mirrors” – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors.

Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures

For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.

In addition, the CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, which were identical to those submitted by the NPPC RSC comments. Please see the SDT's response to RSC NPPC's comments.	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
Oklahoma Gas & Electric supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Vendor remote access is part of remote access. It is not clear why these are separated.	

Additional confusion caused by another SDT will modify the "interactive remote access" definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project. More confusion from the "hall of mirrors" – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, which were identical to those submitted by the NPPC RSC comments. Please see the SDT's response to RSC NPPC's comments.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

N&ST does not agree that the desired clarity has been achieved, especially since for certain types of "vendor remote access," (e.g., Interactive Remote Access to applicable BES Cyber Systems), Intermediate Systems ARE required. Likewise, for user-initiated remote access, vendor or otherwise, to EACMS and PACS systems that happen to be within Electronic Security Perimeters (not altogether uncommon), Intermediate Systems ARE required. N&ST recommends that the SDT consider a more detailed breakdown of R3 requirement applicability to help Responsible Entities distinguish between types of "vendor remote access" that require Intermediate Systems and types of "vendor remote access that do not, as CIP-005 is currently written, require Intermediate Systems:

Intermediate System required: Vendor remote access that meets the current NERC definition of "Interactive Remote Access" and is therefore subject to CIP-005 R2.

Intermediate System not required: Vendor remote access that does not meet the current NERC definition of "Interactive Remote Access." This includes system-to-system remote access and all types of vendor-initiated remote access to EACMS and PACS devices for which CIP-005 R2 is not applicable.

One way to address this might be to break R3 part 3.1 into two sub-parts:

Part 3.1.1 would be applicable to High Impact BES Cyber Systems and their associated PCA as well as Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA (Note the applicability is IDENTICAL to CIP-005 R2).

Part 3.1.2 would be applicable to EACMS and PACS associated with High Impact BES Cyber Systems and with Medium Impact BES Cyber Systems with External Routable Connectivity that are not subject to CIP-005 R2.

Likes 0	
Dislikes 0	

Response	
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The proposed draft does not exclude the use of an Intermediate System for IRA into EACMS or PACS that are logically located within an ESP because those EACMS would by definition be dual classified as Protected Cyber Assets (PCAs) and therefore subject to CIP-005-7 R2 Part 2.1 based on the inclusion of 'associated PCAs' within the Applicable Systems. The Applicable Systems in a given Requirement Part are mutually exclusive of that of another Requirement Part, and the presence of EACMS and PACS in Parts within R3 neither not supersede nor modify the scope of the Applicable Systems in any other Requirement Part. The SDT appreciates that N&ST has proposed some potential language to help clarify where CIP-005-7 R2 is applicable and will consider the suggestions made when preparing the next proposed draft	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No

Document Name	
Comment	
PacifiCorp supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
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 changes which move Vendor Remote Access remote access from Parts 2.4 and 2.5 to Parts 3.1 and 3.2 better clarify the requirements for entities, however adding EACMS to the scope of the standard begs the question if an entity now needs another EACMS Intermediate System to access an EACMS? Because an Intermediate System is already defined as an EACMS (because it provides electronic access), and hence the change requires an entity to deploy a separate Intermediate (EACMS) to access the Intermediate System that provides access to the BCS. The entity must implement another upstream control beyond that EACMS in order to disable the access "to" it, thereby creating another upstream device that qualifies as an EACMS by definition. Personnel (employees, vendors, suppliers, contractors, etc..) need to be defined in CIP-004. Systems (vendor or entity owned and maintained) need to occur in CIP-002. Why not revise CIP-002 and allow entities to define only those systems they use as Intermediate Systems and/or Remote Access? Or vendor systems? Why not revise CIP-004 to address vendors?	

Additionally, Requirement R3 Part 3.2 is a "how" in disguise instead of an objective "what". Another potential solution to consider could be the following: Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability to for a vendor to establish and use remote access". If this were the language, then "terminating established vendor remote access sessions" is one way "how" an entity could meet this objective (although it highlights the gap in the existing draft that terminating established sessions alone may not preclude the re-establishment of another session). This language could also resolve the hall of mirrors because now the entity can define the revocation point that precludes authentication and subsequent use within the layers of EACMS controls, and the "knock at the front door" to the EACMS is no longer "access".

Secondly, the standard does not clearly define what System to System remote access is. A valid definition for system to system remote access needs to be created and added to the Glossary of Terms.

Lastly, Requirement 3 also conflicts with Requirement 1 part 1.3. If a Responsible Entity (RE) determines that a connection to a vendor is needed and has placed the appropriate controls on the appropriate interfaces of its protecting asset(s) (Firewalls, routers, etc..) then the connection is needed. Secondly the RE is responsible for determining if a vendor has adequate security controls in place or has applied mitigations as part of their CIP-013 process for that vendor then the requirement 3 is not needed. Connections made from a vendor (type, duration and need) should be spelled out in the procurement contracts derived out of the CIP-013 processes.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS is not required. The SDT intention is to be clear that an Intermediate System is not required for remote access to EACMS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.

Modifications to CIP-002 and CIP-004 are out of scope of the 2019-03 SAR.

The SDT has considered WAPA's comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap from the use of the word 'terminate', and to add the necessary flexibility for an entity to determine how to meet the security objective.	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	No
Document Name	
Comment	
If intent is to specifically denote that the intermediate systems are not required or in scope it should be specifically stated "Intermediate systems are not required for R3"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	
Comment	
Puget Sound Energy supporte the comments of EEI.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) incorporate by reference the Edison Electric Institute's response to Question 1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
The removal of the term “interactive” and the retention of the terms “remote access” alone do not clearly eliminate the ambiguity regarding intermediate systems. In fact, because the term “remote access” is undefined, the modifications have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply. For this reason, GTC/GSOC do not agree that the proposed revisions makes it clearer that Intermediate Systems are not required. GTC/GSOC further reiterate our previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to GSOC's comments.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
In our opinion the original language in CIP-005-6 stating vendor remote access as system-to-system and interactive is clear and encompassing of all vendor remote access. No change is required to further clarify use of an Intermediate System. However, if further clarification that an Intermediate System is not required I propose the following: "Have one or more methods for determining active vendor remote access sessions (including system-to-system remote access, vendor initiated system-to-system remote access with or without use of an Intermediate System as well as Interactive Remote Access)."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT has considered these suggestions and added clarifying language to CIP-005-7 Requirement R3.	
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	No
Document Name	
Comment	

EEI does not agree that the modifications made to the second draft of CIP-005-7, Requirement R3 clarify that Intermediate Systems are not required. This modification conflicts with Requirement R2, subpart 2.1; which requires the use of Intermediate Systems for all interactive remote access sessions regardless of the source of initiation. Also, the definition of EACMS includes Intermediate Systems. For these reasons, Intermediate Systems cannot be excluded. Moreover, Requirement R3 makes EACMS applicable to this requirement. EEI additionally notes that our comments to the previous draft suggested excluding EACMS from the applicability section of Requirement R2, subpart 2.5. Moving this requirement, along with the minor modifications has not solved the issues identified in our comments to the earlier draft of CIP-005-7.

It is our understanding that "vendor remote access" includes both Interactive Remote Access (IRA) as well as system-to-system access. Consequently, entities would be required to determine the identity of the source of communications before they can establish a session with the Intermediate System, which is not possible because systems must establish a session with the Intermediate System in order to receive user credentials, which are then generally checked with another EACMS (such as a domain controller) in order to determine whether the source is a vendor. At this point, the vendor's system has already had access to the entity's EACMS.

For these reasons, we ask the SDT to consider removing EACMS from the scope of CIP-005 Requirement R3. We understand that the security objective for this requirement is to determine and disable vendor remote access sessions to BES Cyber Systems by using EACMS. If this is incorrect, we ask the SDT to more clearly described the objective.

Likes 0	
Dislikes 0	

Response
The SDT thanks your for your comments, please see response to EEI 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	No
Document Name	

Comment
Vendor remote access is part of remote access. It is not clear why these are separated.

Additional confusion caused by another SDT will modify the "interactive remote access" definition. That update will happen after this update. We recommend this definition of change needs to happen as part of this project. More confusion from the "hall of mirrors" – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The SDT appreciates the security focus that remote access should be treated similarly, however, this is a critical distinction that is necessary, especially in the context of union agreements where an entity could be faced with an impossibility of compliance if required to monitor activity and detection of established of union personnel. Additionally, it stands to reason that vendor remote access, as a function of its risk, be treated differently and more rigorously than remote access by the entity. For these reasons, the SDT was mindful to separate out vendor remote access to assure the activity monitoring and session detection components of vendor access are not extended to an entity's employee base. The Interactive Remote Access (IRA) definition is used pervasively within the CIP Standards and it is out of the SDT scope of the 2019-03 SAR to modify NERC Glossary of Terms definitions that impact CIP Standards outside those that are considered the supply chain risk management Reliability Standards; CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). Additionally, the 2016-02 has a specific directive in their SAR to address the NERC V5-TAG issues, for which IRA is one. For these reasons the SDT has not modified the IRA definition. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate

System for EACMS and PACS is not required. The SDT has elected to keep EACMS and PACS out of Requirement R2 Part 2.1 to prevent confusion of the 'hall of mirrors' and believes the consistency gained by reintroducing EACMS and PACS to Requirement R2 Part 2.1 would not be worth the ambiguity it breeds. For these reasons, SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS or PACS is not required.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
IESO, in general, supports the comments submitted by NPCC and by IRC The wording of Requirement R3 suggests that these are only requirements that apply to vendor initiated remote access and may miss the embedded requirement in Requirement R2. IESO recommends that the wording of Requirement R2 should explicitly add “including vendor initiated interactive remote access” as reminder that there are additional requirements for vendor initiated remote access outside of Requirement R3	

While it is preferred, from a cyber-security perspective, to utilize an intermediate system for vendor initiated interactive remote access to EACMS and PACS, IESO recognizes that it may not be appropriate in all situations	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to NPPC RSC's comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI does not agree that the modifications made to the second draft of CIP-005-7, Requirement R3 clarify that Intermediate Systems are not required. This modification conflicts with Requirement R2, subpart 2.1; which requires the use of Intermediate Systems for all interactive remote access sessions regardless of the source of initiation. Also, the definition of EACMS includes Intermediate Systems. For these reasons, Intermediate Systems cannot be excluded. Moreover, Requirement R3 makes EACMS applicable to this requirement. EEI additionally notes that our comments to the previous draft suggested excluding EACMS from the applicability section of Requirement R2, subpart 2.5. Moving this requirement, along with the minor modifications has not solved the issues identified in our comments to the earlier draft of CIP-005-7.

It is our understanding that "vendor remote access" includes both Interactive Remote Access (IRA) as well as system-to-system access. Consequently, entities would be required to determine the identity of the source of communications before they can establish a session with the Intermediate System, which is not possible because systems must establish a session with the Intermediate System in order to receive user credentials, which are then generally checked with another EACMS (such as a domain controller) in order to determine whether the source is a vendor. At this point, the vendor's system has already had access to the entity's EACMS.

For these reasons, we ask the SDT to consider removing EACMS from the scope of CIP-005 Requirement R3. We understand that the security objective for this requirement is to determine and disable vendor remote access sessions to BES Cyber Systems by using EACMS. If this is incorrect, we ask the SDT to more clearly described the objective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The word "all" in CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. The focus is not limited to vendor remote access through an EACMS into a BCS. The focus also includes vendor remote access into the EACMS or PACS itself, which could ultimately lead to further unauthorized access to the BCS. Otherwise stated with EACMS as the use case, if an entity allows a vendor's untrusted (or less-trusted) system or personnel to remotely connect machine-to-machine or user-to-machine into the entity's EACMS, and the vendor's system is compromised, then that entity must make sure the vendor's compromised system and personnel are no longer connected remotely into the entity's EACMS. The security objective is remove a vendor's ability to retain or reestablish remote access sessions for each of these discrete Cyber Systems: - high impact BES Cyber Systems; - EACMS associated to high impact BES Cyber Systems; - PACS associated to high impact BES Cyber Systems; - medium impact BES Cyber System with External Routable Connectivity; - EACMS associated to medium impact BES Cyber System with External Routable Connectivity; and - PACS associated to medium impact BES Cyber System with External Routable Connectivity.	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Andrea Barclay - Georgia System Operations Corporation – 4	
Answer	No
Document Name	

Comment
The removal of the term "interactive" and the retention of the term "remote access" (now, undefined) alone do not clearly eliminate the ambiguity regarding intermediate systems. In fact, because the term "remote access" is undefined, the modifications have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply as discussed below in GSOC's and GTC comments in response to Question 2. For this reason, GSOC and GTC does not agree that the proposed revisions make it clearer that Intermediate Systems are not required. GSOC and GTC further reiterates its previous comments regarding the unsupported addition of PACS to this requirement.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required. The NERC – Cyber Security Supply Chain Risks, Chapter 2 recommended the 2019-03 SDT to develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards. The SDT considered this recommendation and proposes the modified language in CIP-005-7 Requirement R3 to include PACS as an Applicable System. The SDT affirms its previous response to previous comments and has incorporated this into the Technical Rationale. That response is as follows: The SDT appreciates the thorough nature of comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS: 1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",

2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through
a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore, the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
The NERC definition of Electronic Access Control or Monitoring Systems clearly states that Intermediate Systems are also considered as EACMS. Recommend specific language to address "Electronic Access Point(s)" for system to system remote access and intermediate systems for vendor IRA. It is inferred, however, not clear, that an Intermediate system is not required for system to system access, but is needed for IRA. Separating the two parts into another requirement would make it clearer, however in R2.1 the requirement still reads that for **all** Interactive Remote Access, utilize an intermediate system. Somehow it still creates confusion if it's required for "all" but not for vendors? In Requirement R2, Part 2.1, revise "all" remote sessions must be through an Intermediate System and add "excluding vendor system to system remote access through an EAP." Additionally, the requirement R3 Part 3.1 states "to detect" vendor-initiated remote access sessions. In the Examples of evidence, "Methods for accessing logged or monitoring information…" implies that the Responsible Entity is required to monitor vendor activity during the remote session. Is the objective to detect or to monitor the vendor remote access session or both? For instance, once the vendor remote session is detected or established, is the Responsible Entity required to monitor the vendor activity continuously during the remote session or just receive periodic alerts that the session remains open with the ability to terminate as needed?	

Likes 0	
Dislikes 0	

Response

Thank you for your comments. An Intermediate System is not required for system to system access, but is required for IRA where the Applicable Systems indicates it is required. The word "all" in CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs, and here an Intermediate System is required for IRA. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.

The objective is for the entity to have methods to detect vendor remote access sessions such that if a vendor's system is compromised, and that vendor's untrusted (or less-trusted) system or personnel are (or can) remotely connect machine-to-machine or user-to-machine into the entity's Applicable Systems as cited in each Requirement Part within R3, then that entity must make sure the vendor's compromised system and personnel are no longer connected remotely (or able to reconnect remotely) into the entity's Applicable Systems. Depending on the Requirement Part, this includes 1) remote access by a vendor into the EACMS or PACS; 2) remote access by a vendor that goes through an EACMS into a high impact BES Cyber System and its associated PCAs; and remote access by a vendor that goes through an EACMS into a medium impact BES Cyber System with External Routability and its associated PCAs.

EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS.

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020

Answer	No
Document Name	

Comment
The purpose of CIP-005 is to manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP). The ISO/RTO Council Standards Review Committee (IRC SRC) is supportive of adding PCAs to CIP-005 since PCAs are already defined as a Cyber Asset within an ESP, but EACMS and PACS are not part of the ESP. The concern is that extending the scope of CIP-005 to include EACMS and PACS will require EACMS and PACS to be treated as if they are part of the network inside of the ESP. By definition, Cyber Assets that perform electronic access control or electronic access monitoring of the ESP includes Intermediate Systems and according to the Intermediate Systems definition, an Intermediate System must not be located inside the Electronic Security Perimeter. For these reasons, the IRC SRC is against adding EACMS and PACS for the added scope of network inside of the ESP as the proposed language introduces an unsolvable problem. Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013. Finally, the IRC SRC believes it is too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven.
Likes 0
Dislikes 0
Response
Thank you for your comments. There is no intention, nor implied requirement, for EACMS or PACS to holistically inherit all requirements for BES Cyber Systems, nor is there any requirement to for entities to rearchitect their environment to include EACMS or PACS within an ESP. The Applicable Systems in a given Requirement Part are mutually exclusive of that of another Requirement Part, and the presence of EACMS and PACS in Parts within R3 neither not supersede nor modify the scope of the Applicable Systems in any other Requirement Part. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and

Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within CIP-005-7.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO is supporting the IRC SRC Comments as follows: The purpose of CIP-005 is to manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP). The ISO/RTO Council Standards Review Committee (IRC SRC) is supportive of adding PCAs to CIP-005 since PCAs are already defined as a Cyber Asset within an ESP, but EACMS and PACS are not part of the ESP. The concern is that extending the scope of CIP-005 to include EACMS and PACS will require EACMS and PACS to be treated as if they are part of the network inside of the ESP. By definition, Cyber Assets that perform electronic access control or electronic access monitoring of the ESP include Intermediate Systems and according to the Intermediate Systems definition, an Intermediate System must not be located inside the Electronic Security Perimeter. For these reasons, the IRC SRC is against adding EACMS and PACS for the added scope of network inside the ESP as the proposed language introduces an unsolvable problem. Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013. Finally, the IRC SRC believes it is too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. There is no intention, nor implied requirement, for EACMS or PACS to holistically inherit all requirements for BES Cyber Systems, nor is there any requirement to for entities to rearchitect their environment to include EACMS or PACS within an	

ESP. The Applicable Systems in a given Requirement Part are mutually exclusive of that of another Requirement Part, and the presence of EACMS and PACS in Parts within R3 neither not supersede nor modify the scope of the Applicable Systems in any other Requirement Part. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within CIP-005-7.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
R2.1 states that an Intermediate System is required for all IRA. Vendor access is not excluded. Moving vendor access from Part 2 to Part 3 does not change that R2.1 is required. SRP recommends language in the standards are made clearer to indicate Intermediate Systems are not required in R3	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT has elected to keep EACMS and PACS out of Requirement R2 Part 2.1 to prevent confusion of the 'hall of mirrors' and believes the consistency gained by reintroducing EACMS and	

PACS to Requirement R2 Part 2.1 would not be worth the ambiguity it breeds. For these reasons, SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS or PACS is not required.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to NPPC RSC's comments.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes

Document Name	
Comment	
Duke Energy agrees that the proposed modifications in CIP-005-7 makes it clearer that Intermediate Systems are not required.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree to move all Vendor Remote Access requirement remote access from Parts 2.4 & 2.5 to Parts 3.1 and 3.2 since it is clearer that Intermediate System is not required for Interactive Remote access to EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	

Comment	
The addition of the Applicable Systems to the Requirement Parts (by itself) makes it clear that Intermediate Systems are not required for vendor remote access; some of these applicable systems cannot reside in a defined Electronic Security Perimeter. The term "vendor-initiated" is troubling because it should not matter whether the vendor or the entity initiates the connection; the risks are identical either way. By specifying only "vendor-initiated" connections, the language omits some vendor remote access connections, and therefore does not meet the security objective of the Requirement. WECC recommends removing the term "vendor-initiated" to ensure risks of vendor access connections are addressed, whether vendor or entity initiated.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. Intermediate Systems are required for IRA into the high impact BES Cyber System and its associated PCAs, as well as the medium impact BES Cyber System with External Routable Connectivity and its associated PCAs, including vendor remote access. The SDT has considered concerns about the use of "vendor-initiated" and recognizes that risks may be higher when access is initiated from vendor equipment vs. access initiated from entity owned equipment.	
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	
While this does make it clearer, as a part of the standard's Supplemental Material this should be spelled out, so there is no gray area.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT will revisit supporting material and include clarifying content.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
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	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
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	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	

Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 7 for Northern California Power Agency	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees an additional Intermediate System is not needed for access to an EACMS Intermediate System, and that the SDT's addition of a new Requirement R3 clarifies this fact. Texas RE notes that, as presently drafted, the proposed Requirement R3 does not require multi-factor authentication and encryption for PACS and EACMS. Vendor remote access brings an increased risk of threats and vulnerabilities to registered entities' CIP environments. For example, a malicious actor could gain access to and/or control of the EACMS and PACS for multiple registered entities through a single compromised vendor. Requiring multi-factor authentication and encryption controls would help decrease the risk of misuse, compromise, and data breach through vendor remote access sessions. As such, Texas RE suggests that the SDT consider incorporating multi-factor authentication and encryption requirements into the proposed Requirement R3. Alternatively, the SDT could implement these requirements by adding PACS and EACMS to the Applicable Systems subject to Requirement R2, Parts 2.1 – 2.3, while retaining the proposed Parts 2.4 and 2.5 from Draft One and incorporating clarifying language explaining that when an Intermediate System is an EACMS, another Intermediate System is not required.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT intentionally moved EACMS out of CIP-005-7 R2 in response to significant industry concern regarding the hall of mirrors. EACMS is a term that is pervasively used throughout the CIP Standards, and while the FERC Order directs the SDT to increase the scope of vendor remote access detection, monitoring, and response actions for EACMS, requiring multi-factor authentication and encryption requirements globally for EACMS and PACS may be outside the scope of the 2019-03 SAR and a change the SDT cannot make. The SDT acknowledges Texas REs risk concerns.	

2. The SDT is proposing language in CIP-005-7 in the newly formed R3 to clarify remote session conditions. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. NPCC RSC did not provide comments for Question 2.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
There is no definitive definition of what is an active vendor remote access session including system-to-system remote access as well as Interactive Remote Access, which includes vendor-initiated sessions. SRP would like to see clear definitions added to the Glossary of Terms and examples of each within the Guidelines and Technical Basis.	
Likes 0	

Dislikes 0	

Response
Thank you for your comments. The word 'remote' refers to ‘a lower trust level system external to the Applicable Systems it is connecting into or through’, and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR (formerly known as GTB) to bring further clarity.

Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	

Comment
CIP-005, R3.1 “Detecting” is not a good word choice. Malicious traffic must be detected because it requires investigation and discovery. Vendor remote access is granted by the entity and the entity provides the method by which remote access is performed. The method enabling remote access must have the ability to enumerate remote access sessions. Suggestion: The method enabling vendor-initiated remote access must have the ability to enumerate connected remote access sessions. **CIP-005, R3.2** An “established vendor” is a vendor that has been in business or a long time. How long does a session have to be active before it is widely considered to be established? The intent is to terminate a “connected” session. Suggestion: Have one or more method(s) to terminate connected vendor-initiated remote access sessions.

Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT modified the use of the word "detecting". The SDT has considered concerns about the use of “vendor-initiated” and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT appreciates that Platte River Power Authority has proposed some potential language to help clarify where CIP-005-7 R2 is applicable and will consider the suggestions made when preparing the next proposed draft.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
It isn’t as clear as it could be. Diagrams of the different scenarios would certainly help to clarify. Additionally, suggest replacing the word “Detect” as this implies the vendor is trying to make a remote connection without any permission from the Responsible Entity. Suggested wording for R3, Part 3.1: Have one or more methods for “establishing and monitoring” vendor-initiated remote access sessions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT modified the requirement to remove the use of the 'detecting'. The SDT will also consider diagrams of different scenarios as improvements to the IG and TR to bring further clarity.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
The proposed revisions do not clearly define the types of remote sessions that are covered by the standards and have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply. More specifically, the term "remote access" is not defined and could be construed as access from outside an entity's network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GSOC and GTC does not agree that the proposed revisions makes clearer the types of remote sessions that are covered by the standards. GSOC and GTC recommends that the SDT either: (1) collaborate with the appropriate, assigned SDT to modify the definition of "Interactive Remote Access" as necessary to ensure that it incorporates the necessary language or (2) create newly defined terms for "vendor-initiated remote access" and "vendor-initiated system-to-system access." GSOC and GTC further reiterates its previous comments regarding the unsupported addition of PACS to this requirement.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The word 'remote' is embedded within certain enforceable Glossary of Terms definitions, and it is outside the scope of the 2019-03 SAR to define terms that would have a broader reaching impact outside the scope of the supply chain risk management standards. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	

MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The current language in CIP-005-7, Requirement R3 does not sufficiently describe what constitutes, or clarifies the meaning of, a remote session within the context of an EACMS. Specifically, having access to an EACMS does not mean the device has been exploited.	

Moreover, the term “remote” in the context of an EACMS, such as an Intermediate System, is unclear given Intermediate Systems, by definition, must be remote from an Electronic Security Perimeter.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees that having EACMS access does not mean the EACMS has been exploited. The intent is to mitigate the risk that vendor remote access to an EACMS poses to the associated BES Cyber Systems. The word 'remote' refers to ‘a lower trust level system external to the Applicable Systems it is connecting into or through’, and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
As written, see comments to question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to Question 1 for Independent Electricity System Operator	

Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
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	No
Document Name	
Comment	
The current language in CIP-005-7, Requirement R3 does not sufficiently describe what constitutes, or clarifies the meaning of, a remote session within the context of an EACMS. Specifically, having access to an EACMS does not mean the device has been exploited. Moreover, the term "remote" in the context of an EACMS, such as an Intermediate System, is unclear given Intermediate Systems, by definition, must be remote from an Electronic Security Perimeter.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments, which were identical to those submitted by the EEI comments. Please see the SDT's response to EEI's comments.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
See response to question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Refer to the SDT's response to Question 1 for Ameren - Ameren Services	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what “vendor-initiated” actually is. It would be beneficial to leverage language of Interactive Remote Access such as “Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)”.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. It is not the intention of the SDT to expand the context of remote sessions. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity. The SDT appreciates that Lower Colorado River Authority proposed suggestions to help bring clarity. The SDT considered these suggestions when preparing the 3rd draft. The 2016-02 SDT is in the process of proposing revisions to the term Interactive Remote Access (IRA) in order to address NERC V5-TAG issues, and virtualization which proposes to replace existing ESP/EEP concepts with 'logical isolation' to enable the use of emerging technologies while maintaining backwards compatibility. For these reasons, the 2019-03 SDT has chosen not to create a variant to a currently defined term that is undergoing modification and is also perceived by many as ambiguous today in favor of clarifying language within the Applicable Systems and requirement language.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
The proposed revisions do not clearly define the types of remote sessions that are covered by the standards and have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply. More specifically, the term "remote access" is not defined and could be construed as access from outside an entity's network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GTC/GSOC do not agree that the proposed revisions makes clearer the types of remote sessions that are covered by the standards. GTC/GSOC further reiterate our previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to GSOC's comments.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) incorporate by reference the Edison Electric Institute's response to Question 2.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	
Comment	
Puget Sound Energy supporte the comments of EEI.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks your for your comments, please see response to EEI Comments.	
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 term "detecting" in part 3.1 - whereas an entity is required to "Have one or more methods for **detecting** vendor-initiated remote access sessions" implies an entity is not aware of the instances of when a vendor is remotely accessing their BCS and must "detect" when they access the BCS. What is the security value in detecting a vendor who is already authorized to access the BCS?

A person accessing a system, vendor, or other should be addressed in CIP-004. The identification of a vendor system should occur in CIP-002. This also maps to ISO and NIST cyber security frameworks.

Recommend considering preventive controls to authenticate vendor sessions. This could be administrative processes such as sharing a code word, verifying vendor change ticket numbers, pre-confirmed call-out lists, confirming an authentication code (such as RSA token), or technical controls such as Identity and Access Management controls. In some emergency situations a need may arise for vendors to initiate and establish remote access to an entities BCS, however a voice call to authenticate may be a better control.

Secondly, the words "established sessions" are an improvement from the language in the first draft; however, while this solved the problem posed by "disabling active sessions" where an idle session could remain enabled, it created another gap through the introduction of the word "initiated". The qualifier "initiated" may have unintended consequences that defy the security objectives. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access, retention of established sessions, and the ability to re-establish sessions (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the "presence of" and "capability to use" the established session that is the risk regardless of which end initiated it.

Recommend alternative language that focuses on the risk itself or consider: Requirement R3 Part 3.1. "Have one or more methods for detecting established vendor remote access sessions." Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability for a vendor to establish and use remote access". In this case "terminating established vendor remote access sessions" is one way "how" an

entity could meet this objective (although it highlights the gap in the existing draft that terminating an established session alone may not preclude the re-establishment of another session), hence the need to adjust this language. Additionally, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of read-only “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). Consequently, established non-persistent read only sessions (i.e. WebEx) between a Registered Entity and a vendor are being lumped into the “vendor remote access” bucket. Consider language to exclude non-persistent read only information sharing sessions (i.e. WebEx) from being considered “access” to prevent CIP-011 from creeping into CIP-005	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Modifications to CIP-002 and CIP-004 are out of the scope of the 2019-03 SAR. The SDT considered the comment on use of the word 'detecting' and has modified the standard to remove "detecting” The SDT also made additional changes to CIP-005 R3 to address the questions around "established sessions". Finally, the SDT considered the change of adding "vendor initiated" and understands that risk may be different when remote access is started from vendor equipment vs. entity equipment.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports EEI comments.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what “vendor-initiated” actually is. It would be beneficial to leverage language of Interactive Remote Access such as “Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)”.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. James Baldwin submitted identical comments. Please see the SDT's response to Lower Colorado Authority's comments submitted by James Baldwin.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST does not agree that the desired clarity has been achieved. N&ST recommends that the SDT consider a more detailed breakdown of R3 requirement applicability to help Responsible Entities distinguish between types of "vendor remote access" that DO require Intermediate Systems and types of "vendor remote access that do NOT, as CIP-005 is currently written, require Intermediate Systems: Intermediate System required: Vendor remote access that meets the current NERC definition of "Interactive Remote Access" and is therefore subject to CIP-005 R2. Intermediate System not required: Vendor remote access that does not meet the current NERC definition of "Interactive Remote Access." This includes system-to-system remote access and all types of vendor-initiated remote access to EACMS and PACS devices for which CIP-005 R2 is not applicable. One way to address this might be to break R3 part 3.1 into two sub-parts: Part 3.1.1 would be applicable to High Impact BES Cyber Systems and their associated PCA as well as Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA (Note the applicability is IDENTICAL to CIP-005 R2). Part 3.1.2 would be applicable to EACMS and PACS associated with High Impact BES Cyber Systems and with Medium Impact BES Cyber Systems with External Routable Connectivity that are not subject to CIP-005 R2.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. N&ST's comments for Question 2 were identical to the comments submitted for Question 1. Please refer to the SDT's response to N&ST's comment for Question 1.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
As written, see comments to question 1	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 1 for Eversource Energy	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	

Answer	No
Document Name	
Comment	
Oklahoma Gas & Electric supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
As written, see comments to question 1	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 1 for Hydro-Qubec Production.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	

The proposed revisions do not clearly define the types of remote sessions that are covered by the standards. CIP standards need to use consistent language, define unclear terms and not leave so much to interpretation if requiring specific actions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Refer to responses to Question 1.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Refer to the SDT's response to Question 1 for Cogentrix Energy Power Management, LLC	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern does not agree that the changes clearly define the types of remote sessions. There is still some ambiguity on what would be considered remote if the entity is to disable remote access to the very things that are used to define what remote access actually is. Would a remote user who attempts to get to an asset but is not authenticated and authorized, but made it to the asset that denies access, is that still considered access? The security which denies the access, such as a firewall, simply does not allow the access. However, there would be a log that is collected of the attempted access as well as any access that is authenticated and authorized.	
Likes 0	
Dislikes 0	
Response	
CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS.	

The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to Tacoma Power's comments.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
The proposed changes do not provide clarity. Although the addition of "initiated" is appreciated, the removal of the IRA and system-to-system qualifiers introduces ambiguity. It is unclear whether "all" remote access sessions must be included or if the Entity has the authority to define "vendor-initiated remote access sessions," potentially reducing the scope of requirement. The removal of IRA and system-to-system is also inconsistent with the language changes to CIP-013-2, R1.2.6.	

Additionally, the "Measures" were not updated to reflect the proposed changes. Specifically, the "Measures" still include the language from the original CIP-005-2 R2.4 and R2.5 requirements "active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access." ISO-NE recommends keeping the "initiated" qualifier, adding terms or information to clarify the specific in-scope remote access sessions, and ensuring consistency with CIP-013-2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT moved the IRA and system to system access qualifiers out of the requirement language and into the measures in CIP-005-7 Requirement R3 to address a perceived concern of a 'hall of mirrors'. The SDT has considered concerns about inconsistencies between the language in CIP-013-2 and CIP-005-7 as well as the Measures and has worked to align that language.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
LaTroy Brumfield - American Transmission Company, LLC - 1	

Answer	No
Document Name	
Comment	

ATC agrees the words "established sessions" are an improvement from the language in the first draft; however, while this solved the problem posed by "disabling active sessions" where an idle session could remain enabled, it created another gap through the introduction of the word "initiated". The qualifier "initiated" may have unintended consequences that defy the security objectives. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access, retention of established sessions, and the ability to re-establish sessions (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the "presence of" and "capability to use" the established session that is the risk regardless of which end initiated it. ATC requests consideration of alternative language that focuses on the risk itself. Another potential solution to consider could be the following: Requirement R3 Part 3.1. "Have one or more methods for detecting established vendor remote access sessions." Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability for a vendor to establish and use remote access". If this were the language, then "terminating established vendor remote access sessions" is one way "how" an entity could meet this objective (although it highlights the gap in the existing draft that terminating an established session alone may not preclude the re-establishment of another session), hence the need to adjust this language.

Additionally, the phrase "vendor remote access" is ambiguous because it is undefined and the word "access" is broad. As a result, emerging interpretations are blending the concepts of read-only "information sharing" sessions (CIP-011) with the concepts of BCS "access" sessions (CIP-005 & CIP-007). Consequently, established non-persistent read only sessions (i.e. WebEx) between a Registered Entity and a vendor are being lumped into the "vendor remote access" bucket. ATC requests consideration of qualifying language to exclude non-persistent read only information sharing sessions (i.e. WebEx) from being considered "access" to prevent CIP-011 from creeping into CIP-005.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT appreciates that it has proposed some potential language to address this concern and considered those suggestions when preparing the 3rd draft. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to Tacoma Power's comments.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	

Oncor supports the comments submitted by EEI. In addition, there is a conflict between the language in CIP-005-7, R3 and CIP-013-2 inasmuch CIP-013, R1.2.6 takes out "Interactive", and "with a vendor" in terms of remote or system to system access, but then the changes to CIP-005-7 do not match the changes in CIP-013-2, R1.2.6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to EEI's comments.	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	No
Document Name	
Comment	
As written, see comments to question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 1 for Con Ed - Consolidated Edison Co. of New York.	
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	No
Document Name	
Comment	

The changes to the newly formed R3 appear to have had the opposite effect of clearly defining the types of remote sessions. With these changes, there is no clarity about what a vendor-initiated remote access session is. Does “access” refer to read-only access? Or does “access” only refer to control? What is the meaning of “remote” in this situation? “Remote” to an applicable system? How is that clarified? Tacoma Power does not support these changes to CIP-005 and recommends creating one or more defined terms to help provide clarity in this situation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of “vendor-initiated” and recognizes the risks may be different based on the use of vendor equipment vs entity equipment. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The word 'remote' refers to ‘a lower trust level system external to the Applicable Systems it is connecting into or through’, and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

While the SDT is coming at this from the supply chain aspect, the technical application of the mechanisms to detect, terminate and disable remote access sessions requires the ability to do it for any remote access session; therefore the specific language "active vendor remote access" and "includes vendor-initiated sessions" is of no practical value. If the entity has the ability to detect, terminate, and disable remote access sessions, they have the ability do this for vendors or for insiders. In BPA's opinion, there is no point in making the requirement strictly about vendors. It could as easily be applied to partners, customers, remote employees, etc., and to the same benefit in reduced risk to the reliability and secure operation of the grid.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT appreciates the security focus that remote access should be treated similarly, however, this is a critical distinction that is necessary, especially in the context of union agreements where an entity could be faced with an impossibility of compliance if required to monitor activity and detection of established of union personnel. Additionally, it stands to reason that vendor remote access, as a function of its risk, be treated differently and more rigorously than remote access by the entity. For these reasons, the SDT was mindful to separate out vendor remote access to assure the activity monitoring and session detection components of vendor access are not extended to an entity's employee base.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
No, Santee Cooper does not believe that the changes in CIP-005-7 R3 clarify remote session conditions. If this is the SDT's intent, then they should define vendor-initiated remote access. In CIP-013-2 two different remote access conditions are mentioned vendor-initiated remote access and system to system remote access. Whereas in CIP-005-7 only vendor-initiated remote access is mentioned.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT moved the IRA and system to system access qualifiers out of the requirement language and into the measures in CIP-005-7 Requirement R3 to address a perceived concern of a 'hall of mirrors'. The SDT has considered concerns about inconsistencies between the language in CIP-013-2 and CIP-005-7 and has worked to align that language.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The current language in CIP-005-7, Requirement R3 does not sufficiently describe what constitutes, or clarifies the meaning of, a remote session within the context of an EACMS. Specifically, having access to an EACMS does not equate to the device being exploited. Moreover, the term “remote” in the context of an EACMS, such as an Intermediate System, is unclear given Intermediate Systems, by definition, must be remote from an Electronic Security Perimeter.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, which were identical to those submitted by the EEI comments. Please see the SDT's response to EEI's comments.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE supports the comments as submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments	

The term “detecting” in part 3.1 - whereas an entity is required to “Have one or more methods for **detecting** vendor-initiated remote access sessions” implies an entity is not aware of the instances of when a vendor is remotely accessing their BCS and must “detect” when they access the BCS. What is the security value in detecting an entity which is assumed to already be authorized to access the BCS? Recommend considering preventive controls to authenticate vendor sessions. This could be administrative processes such as sharing a code word, verifying vendor change ticket numbers, pre-confirmed call-out lists, confirming an authentication code (such as RSA token), or technical controls such as Identity and Access Management controls. In some emergency situations, a need may arise for vendors to initiate and establish remote access to an entity's BCS, however, a voice call to authenticate may be a better control. Secondly, the words “established sessions” are an improvement from the language in the first draft; however, while this solved the problem posed by “disabling active sessions” where an idle session could remain enabled, it created another gap through the introduction of the word “initiated”. The qualifier “initiated” may have unintended consequences that defy the security objectives. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access, retention of established sessions, and the ability to re-establish sessions (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the “presence of” and “capability to use” the established session that is the risk regardless of which end initiated it. Recommend alternative language that focuses on the risk itself or consider: Requirement R3 Part 3.1. “Have one or more methods for detecting established vendor remote access sessions.” Requirement R3 Part 3.2. “Have one or more method(s) to revoke the ability for a vendor to establish and use remote access”. In this case “terminating established vendor remote access sessions” is one way “how” an entity could meet this objective (although it highlights the gap in the existing draft that terminating an established session alone may not preclude the re-establishment of another session), hence the need to adjust this language. Additionally, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of read-only “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). Consequently, established non-persistent read-only sessions (i.e. WebEx) between a Registered Entity and a vendor are being lumped into the “vendor remote access” bucket. Consider language to exclude non-persistent read-only information sharing sessions (i.e. WebEx) from being considered “access” to prevent CIP-011 from creeping into CIP-005.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. Modifications to CIP-002 and CIP-004 are out of the scope of the 2019-03 SAR. The SDT modified the used of the word 'detecting' in CIP-005 R3. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different with the use of vendor equipment vs entity equipment. The SDT appreciates that MRO NSRF has proposed some potential language to help clarify where CIP-005-7 R2 is applicable and will consider the suggestions made when preparing the next proposed draft. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT will also consider improvements to the IG and TR to bring further clarity.

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

Comment
No, the changes made it worse by including the definition of a session in the measure and not in the requirement itself. As written in part 3.1 entities have to detect "vendor-initiated remote access sessions" without indication on what this includes. It is vague language. In the measure a definition is given for an active vendor remote access session as "including system-to-system, as well as interactive remote access, which includes vendor-initiated sessions". Requirements cannot be buried in glossary definitions or measures as it implies a rule without be an explicit rule. The definition needs to be placed back into the requirement itself.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT moved the IRA and system to system access qualifiers out of the requirement language and into the measures in CIP-005-7 Requirement R3 to address a perceived concern of a 'hall of mirrors'.

The SDT has considered concerns about inconsistencies between the language in CIP-013-2 and CIP-005-7 as well as the Measures and has worked to align that language. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
The Measures detailed in the Requirement Parts do clearly define the types of remote sessions that are covered by the standards. However, the Measures language does not use the same terminology ("vendor-initiated" connections) that is used in the Requirements language, which may lead to confusion. WECC recommends removing the term "vendor-initiated" as discussed in the previous comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT has considered concerns about inconsistencies between the language in CIP-013-2 and CIP-005-7 as well as the Measures and has worked to align that language.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State does find the addition of the phrase "vendor-initiated" helpful, however we think it still leaves too much room for interpretation. To further clarify, we recommend a few additional edits: 1) In the measure for part 3.1, recommend changing the language "(including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)" with "(either via system-to-system remote access or Interactive Remote	

Access, and which is initiated from a vendor's asset or system)", and 2) In the requirement itself, we recommend adding something like the following to end of the drafted requirement language ", whether via system-to-system remote access or Interactive Remote Access." Similar edits should be made to part 3.2. Finally, we ask that the drafting team consider adding a statement to help clarify and address the various emerging regional interpretations regarding web conferences, either in the core requirement R3, or under both parts 3.1 and 3.2. To that end, we recommend adding a statement to this effect "Remote sessions initiated by the responsible entity's personnel, where the vendor has no control, is not in scope".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline

within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

The words "vendor-initiated remote access sessions" are not properly defined and are ambiguous. "Sessions" could be taken as exclusive to TCP Only connections or could mean any connection such as a serial HyperTerminal session … etc.

R2 strictly discusses vendor-initiated remote access. If an entity initiates the remote access via a WebEx and gives control to a vendor the access should then be considered vendor initiated and follow R3 requirements.

Does the vendor-initiated remote access include non-routable vendor-initiated communications Consider including communications such as dial-up, serial, corporate TTY terminal servers to EACMS and PACS, etc. Perhaps modify requirements to state P3.1 – " Have one or more methods for detecting all vendor sessions, regardless of protocol, type of connection, or initiation" and P3.2 - "Have one or more methods to terminate all vendor sessions regardless of protocol, type of connection, or initiation"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks could be higher from vendor equipment vs entity equipment. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Erick Barrios - New York Power Authority - 6	
Answer	No
Document Name	
Comment	
As written, see comments to question 1.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Refer to the SDT's response to Question 1 for New York Power Authority.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not agree that the proposed language clarifies remote session conditions. Duke Energy, is concerned about the new wording for R3.1, specifically the change of “determined” to “detecting”. This leaves open a question if the intent is continuous monitoring for or detection of sessions, on-demand or periodic detection, or just detection upon initiation.	
Likes 0	
Dislikes 0	
Response	
The SDT modified the use of the word ‘detecting'.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO is supporting the IRC SRC Comments as follows: The IRC SRC believes that the proposed language under R3 more clearly defines the type of remote sessions that are covered by adding "vendor-initiated…".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Though CAISO supported the addition of 'vendor-initiated', the SDT received several industry comments with concerns regarding the addition of 'initiated' and the SDT considered those comments.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	Yes
Document Name	

Comment	
The IRC SRC believes that the proposed language under R3 more clearly defines the type of remote sessions that are covered by adding "vendor-initiated…"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Though MISO supported the addition of 'vendor-initiated', the SDT received several industry comments with concerns regarding the addition of 'initiated' and the SDT considered those comments.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Snohomish County PUD No. 1 did not provide comments for Question 2.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree to the proposing language in Part 3.2, but disagree the term “detecting” in Part 3.1 since “detecting” implies an entity is not aware of the instances of when a vendor is remotely accessing their BCS and must “detect” them. We suggest changing from “detecting” to “verifying”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has modified the requirements to remove the 'detecting'. This aligns with the FERC Order to extend protections to EACMS and PACS without modifying the original intent of the Requirement.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
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	

Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
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	

Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments to #1.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	

Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	

Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 7 for Northern California Power Agency.	

3. The SDT is proposing removing the exception language in CIP-010-4 "Applicable Systems" for PACS which stated "except as provided in Requirement R1, Part 1.6." This reverts the language in this section back to what is in CIP-010-3. Do you agree with this proposed modification? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented

on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.	
Likes 0	
Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

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

Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Question does not address the proposed addition of EACMS and PACS to the CIP-10-3 R1.6 requirement. ISO-NE does not agree with adding EACMS and PACS to the "Applicable Systems." The additions potentially exceed the FERC order, which can be interpreted to only extend the supply chain requirements to the CIP-013-1 Standard. Given the CIP-010-3 R1.6 requirement is not even effective yet, there is insufficient evidence to support further expansion into a CIP environment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards..." Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security –	

Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within both CIP-005-7 and CIP-010-4.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC/GSOC do not support any revisions that have the result of including PACS in the requirements of interest in this project. Various reliability standards already mitigate security risks relating to PACS, e.g., CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GTC/GSOC assert that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GTC/GSOC oppose the inclusion/addition of PACS to the supply chain reliability standards. While GTC/GSOC understand the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, they believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to GSOC's comments.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	

Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC and GTC does not support any revisions that have the result of including PACS in the requirements of interest in this project. Various reliability standards already mitigate security risks relating to PACS, e.g., CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GSOC and GTC asserts that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GSOC and GTC remains opposed to the inclusion/addition of PACS to the applicable supply chain reliability standards. While GSOC and GTC understands the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, we believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.	
Likes 0	
Dislikes 0	
Response	
The SDT appreciates the thorough nature of comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS: 1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.", 2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and	

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through

a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore,

the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	No
Document Name	
Comment	
The IRC SRC believes the question should solicit comment as to the proposed addition of EACMS and PACS of draft 1 which we oppose. Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013. Also, too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven. The IRC SRC believes that requirement R1.6 should be applied to other Cyber Assets. Making a regulatory compliance requirement for a subset of assets in the enterprise increases the cost of implementation and maintenance dramatically to a point that it may be detrimental to the overall company security posture, ultimately increasing the security risk to the company. Therefore, the IRC SRC opposes adding EACMS and PACS to the R1.6 requirement as this requirement has not yet proven to be effective as it stands.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with	

medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within both CIP-010-4 and CIP-005-7.

The SDT appreciates the comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:
1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".
In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.
The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.
Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect. Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

CAISO is supporting the IRC SRC Comments as follows:

The IRC SRC believes the question should solicit comment as to the proposed addition of EACMS and PACS of draft 1 which we oppose.

Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013.

Also, it is too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven.

it also believes that regulatory requirements should not be applied to additional Cyber Assets. When a regulatory compliance requirement is expanded to include additional assets in the enterprise, it increases 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. Therefore, the IRC SRC opposes adding EACMS or PACS to the supply chain requirement as this requirement has not yet proven to be effective as it stands.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within both CIP-010-4 and CIP-005-7.

The SDT appreciates the comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:
1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".
In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk. Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect. Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves. The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore, the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with reverting the language in this section back to what is in CIP-010-3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree to remove the specific language in the Background section to clarify the applicable PACS.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments.	
Erick Barrios - New York Power Authority - 6	
Answer	Yes
Document Name	
Comment	
The redline-to-last-posted does not show any changed to Part 1.6. We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments Removing this specific language helps entities to clarify the requirements pertaining to each applicable system.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Snohomish County PUD No. 1 did not provide comments for Question 3.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

BPA agrees that this reads better with the language removed. However, if we are looking at this from a Supply Chain perspective perhaps we should consider removing with "External Routable Connectivity" and evaluate all PACS as they are being procured.	
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, and the removal of ERC would have broad ranging impacts to the suite of CIP Cyber Security Standards and is not in scope for the 2019-03 SAR.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	

The redline-to-last-posted does not show any changed to Part 1.6. We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
No additional comments on this question.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment	
Southern does not have any issues with the removal of the exception language in the Applicable Systems for PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Answer should have been "No". We do not su[pport adding PACS.	
Likes 0	
Dislikes 0	
Response	
he SDT appreciates the comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS: 1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.", 2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and	

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through
a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore,

the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
The redline-to-last-posted does not show any changed to Part 1.6 We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

The redline-to-last-posted does not show any changed to Part 1.6 We agree that the SDT followed the Directive's instructions	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	
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	
Removing this specific language helps entities to clarify the requirements pertaining to each applicable system.	
Likes 0	
Dislikes 0	
Response	
Thank 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	
The redline-to-last-posted does not show any changed to Part 1.6. We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Leonard Kula - Independent Electricity System Operator - 2	

Answer	Yes
Document Name	
Comment	
We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
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	
Steven Rueckert - Western Electricity Coordinating Council - 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	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
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	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
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	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 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	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
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	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
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	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment, please see respond to question 7.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	

Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments	

4. To address comments the SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 to clarify that all types of vendor-initiated remote access needs to be considered. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendations and if appropriate, technical or procedural justification.

Cyber Security Supply Chain Risk Standard Drafting Team Summary Response:

CIP-013-2 is a risk-based standard that requires an Entity to develop and implement a supply chain cyber security risk management plan. The Entity's plan should include process(s) for procurement that address minimum requirements listed in R1.2.1-R1.2.6. This requirement is about a plan and ensuring the controls are coordinated between the Entity and the Vendor, and is intentionally not prescriptive in order to allow the Entity enough flexibility in developing their specific plan(s) and process(es).

CIP-005-7 3.1 and 3.2 language has been updated. CIP-13-2 R2.1.6 also has been updated to clarify vendor-initiated remote access, and more closely align with the new proposed revisions to CIP-005-7.

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to NPCC RSCC.	

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
There is no clear definition of what is a vendor-initiated, remote access and system-to-system remote access. SRP would like to see the definitions clearly defined.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO is supporting the IRC SRC Comments as follows: The IRC SRC believes that the reconstructed wording of requirement R1, Part 1.2.6 is inconsistent with the proposed changes to CIP-005. It is not clear of what types of remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	No
Document Name	
Comment	
The IRC SRC believes that the reconstructed wording of requirement R1, Part 1.2.6 is Inconsistent with the proposed changes to CIP-005. It is not clear of what types of remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	
Removing "Interactive" creates ambiguity and negates the need for having a (i) and (ii). The result is (i) remote access, and (ii) system-to-system remote access (which is a subset and included within (i) remote access). Without "Interactive" (ii) is redundant. The resulting requirement then would be, "Coordination of controls for vendor-initiated remote access". The term "remote access" is unclear and must be further defined. That is why the original language clarified "remote access" using "Interactive Remote Access" (a defined term) and "system-to-system remote access" (commonly understood). Suggestion: define the term "remote access" or put "Interactive Remote Access" and "system-to-system remote access" back into the requirement.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
This creates more confusion as CIP-005-7 refers to IRA and vendor remote access. Need to correlate that if the vendor uses IRA, requirements in R2 apply. Correct? Otherwise vendor remote access (system to system) must be through an EAP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
For the reasons indicated above, GSOC and GTC respectfully reiterates that revisions to strip the requirements down to generic terms like "remote access" and "system to system access" have the potential to be construed as broadening the potential interpretation of the types of remote access sessions to which the requirements would apply. More specifically, the terms "remote access" and "system to system access" are not defined and, even as modified by the term "vendor-initiated," could be construed as access from outside an entity's network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate	

system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GSOC and GTC does not agree that the proposed revisions make clearer the types of remote sessions that are covered by the standards. GSOC and GTC further reiterates its previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican Energy Company agrees with considering vendor-initiated remote access. However, the standard language should address the intent versus the capability. Further, we recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the version proposed. Even if the vendor could potentially gain access, such as by requesting control during a WebEx meeting, that is not vendor-initiated remote access. Examples: • If the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. • If the intent is to show a user's computer for trouble-shooting or other reasons, then this is read-only access managed by the Entity and not subject to the standard.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican Energy Company agrees with considering vendor-initiated remote access. However, the standard language should address the intent versus the capability. Further, we recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the version proposed. Even if the vendor could potentially gain access, such as by requesting control during a WebEx meeting, that is not vendor-initiated remote access. Examples: · If the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. · If the intent is to show a user's computer for trouble-shooting or other reasons, then this is read-only access managed by the Entity and not subject to the standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
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 recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We believe that the proposed wording changes for R1.2.6 unnecessarily broaden the scope of this requirement. The term "interactive" is key to the wording of this requirement and consistent with the usage of IRA elsewhere in the CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	

The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what "vendor-initiated" actually is. It would be beneficial to leverage language of Interactive Remote Access such as "Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
For the reasons indicated above, GTC/GSOC respectfully reiterate that revisions to strip the requirements down to generic terms like "remote access" and "system to system access" have the potential to be construed as broadening the potential interpretation of the types of remote access sessions to which the requirements would apply. More specifically, the terms "remote access" and "system to system access" are not defined and could be construed as access from outside an entity's network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GTC/GSOC do not agree that the proposed revisions makes clearer the types of remote sessions that are covered by the standards. GTC/GSOC further reiterate our previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the SDT's summary response under question 4.	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	No
Document Name	
Comment	
To enhance general applicability to all vendor-initiated remote access, suggest: "Coordination of controls for all vendor-initiated remote access." We believe that specifying and breaking down remote access types (e.g. "system to system") adds confusion and decreases clarity with respect to securing all manners of vendor-initiated remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
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	
Without a definition of what System to System remote access is, the changes requested do nothing to clarify anything different that was written in version 2. A definition for system to system remote access needs to be created and added to the Glossary of terms. While this revision clarifies the considerations for remote access controls in supply chain risk management plans and processes, the use of the word "initiated" may have unintended consequences that defy the security intent. The goal is to implement controls that prevent or mitigate the risk of unauthorized access (whether interactive or system-to-system) by a remote vendor then the initiator of that	

established session is moot. It is the "presence of" the established session that is the risk regardless of which end initiated it once the Registered Entity determines that vendor should no longer have that access. Recommend language that focuses on the risk itself. Similar, the phrase "vendor remote access" is ambiguous because it is undefined and the word "access" is broad. As a result, emerging interpretations are blending the concepts of "information sharing" sessions (CIP-011) with the concepts of BCS "access" sessions (CIP-005 & CIP-007). This is evident where established read only sessions between a Registered Entity and the vendor are included as "vendor remote access." Recommend language to exclude established non-persistent read only sessions (i.e. WebEx) from being considered "access" to applicable systems to prevent CIP-011 from creeping into CIP-013 where the scope is supposed to be limited to high and medium impact BES Cyber Systems and their associated EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the notion that vendor-initiated remote access should be considered. We feel that the standard language needs to address capability versus intent of the remote access. Meaning, if the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. This kind of remote access can be contemplated during contract scoping discussions. If a vendor has the capability of implementing changes on a BCS shifts because the vendor is participating in an activity where control of the user's computer could be granted to the vendor (WebEx for example), then this isn't classified as vendor-initiated remote access with regards to the objective of the standard. We recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the current version proposed.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what "vendor-initiated" actually is. It would be beneficial to leverage language of Interactive Remote Access such as "Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)".	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST does not agree that the desired clarity has been achieved. N&ST recommends simplifying Part 1.2.6 to read: "Coordination of controls for vendor-initiated remote access to applicable systems."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the SDT's summary response under question 4.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. . We recommend consistency between these Standards and defining terms such as "interactive remote access" and "remote access".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We do not agree that the proposed language clearly defines the intended types of vendor remote access. First, we do not agree that Interactive Remote Access vendor sessions should be treated differently than internal sessions. Second, Part 1.2.6 (ii) specifies system-to-system remote access but the language is not bound to vendors. The requirement could be interpreted to include all system-system remote access, vendor or internal.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern does not agree with the reconstructed wording. The updated text causes further confusion from the original. During the WebEx it was discussed that IRA and system-to-system are sub-sets of vendor remote access. To ensure clarity, Southern would like the SDT to consider the following possible rewording: "Coordination of controls for vendor-initiated (i) Interactive Remote Access, and (ii) system-to-system remote access to BES Cyber Systems. Another requirement for consideration would be to add the following, "1.2.7 Coordination of controls for vendor-initiated remote access (interactive user access and system-to-system access) to applicable EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE recommends review of the proposed CIP-005-3 changes to ensure consistency.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy supports the notion that vendor-initiated remote access should be considered in CIP-013-2 R1, P1.2.6; however, we feel that the standard language needs to address the capability of the vendor while having access versus the intent of the vendor's remote access. Meaning, if the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. This kind of remote access can be contemplated during contract scoping discussions. However, there is an ambiguity when it comes to the remote sharing applications between Entity and Vendor (i.e. webEX, Skype, Zoom, etc.), in that during these remote sharing events, a user's (Entity) computer can grant to the vendor control of their screen. NV Energy believes that this event isn't classified as vendor-initiated remote access with regards to the objective of the standard. We recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the current version proposed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	

Comment	
The use of the word “initiated” may have unintended consequences that defy the security intent. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the “presence of” the established session that is the risk regardless of which end initiated it once the Registered Entity determines that vendor should no longer have that access. ATC requests consideration of alternative language that focuses on the risk itself. Additionally, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). Consequently, established read only sessions between a Registered Entity and the vendor are being lumped into the “vendor remote access” bucket. ATC requests consideration of qualifying language to exclude established non-persistent read only sessions (i.e. WebEx) from being considered “access” to applicable systems to prevent CIP-011 from creeping into CIP-013 where the scope is supposed to be limited to high and medium impact BES Cyber Systems and their associated EACMS and PACS	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT’s summary response under question 4.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
While the SDT does a good job in reconstructing the wording, it only addresses “’vendor” and “system-to-system” access. Remote access to BES Cyber Assets and Systems can be granted by the entity to not only its employees, but to its vendors and contractors, separate and outside from access granted to other vendors or systems.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
It is better to use the defined terms that are used throughout the standards. Using "remote access" instead of "Interactive Remote Access" implies what is being addressed in this requirement different than Interactive Remote Access in ways other than being vendor-initiated. Also, the source of initiation is not clear with system-system remote access, but if a vendor is compromised, any system-to-system remote access with that vendor should be terminated without regard to who initiated it. The original language is better.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
To enhance general applicability to all vendor-initiated remote access, suggest: "Coordination of controls for all vendor-initiated remote access." We believe that specifying and breaking down remote access types (e.g. "system to system") adds confusion and decreases clarity with respect to securing all manners of vendor-initiated remote access.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
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	No
Document Name	
Comment	
The changes to CIP-013-2 Part 1.2.6 appear to have had the opposite effect. Now there is no clarity about what a vendor-initiated remote access session is. Does "access" refer to read-only access? Or does "access" only refer to control? What is the meaning of "remote" in this situation? "Remote" to an applicable system? How is that clarified?	

Additionally, it appears that (ii) system-to-system remote access, is now just a subset of (i) remote access. Tacoma Power does not support these changes to CIP-013 and recommends creating one or more defined terms to help provide clarity in this situation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes "Coordination of controls" remains somewhat ambiguous. Inclusion of "vendor-initiated" for both remote access and system-to-system remote access is somewhat redundant and confusing. BPA proposes the following: *1.2.6. Coordination of remote access controls for vendor personnel or systems accessing BES Cyber Systems ESP/ESZ to include; reasons and requirements for remote access, periodicity of access (temporary or permanent), methods of authentication, and revocation processes for personnel.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No

Document Name	
Comment	
The SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 that all types of vendor-initiated remote access need to be considered then the wording used in CIP-005-7 should be consistent with the wording used in CIP-013 R1, Part 1.2.6. In CIP-005 "vendor initiated remote access" is used while both "vendor initiated remote access" and system to system remote access is used in CIP-013 R1, Part 1.2.6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	

Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments While this revision clarifies the considerations for remote access controls in supply chain risk management plans and processes, the use of the word "initiated" may have unintended consequences that defy the security intent. The goal is to implement controls that prevent or mitigate the risk of unauthorized access (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the "presence of" the established session that is the risk regardless of which end initiated it once the Registered Entity determines that vendor should no longer have that access. Recommend language that focuses on the risk itself. Similar, the phrase "vendor remote access" is ambiguous because it is undefined and the word "access" is broad. As a result, emerging interpretations are blending the concepts of "information sharing" sessions (CIP-011) with the concepts of BCS "access" sessions (CIP-005 & CIP-007). This is evident where established read-only sessions between a Registered Entity and the vendor are included as "vendor remote access." Recommend language to exclude established non-persistent read-only sessions (i.e. WebEx) from being considered "access" to applicable systems to prevent CIP-011 from creeping into CIP-013 where the scope is supposed to be limited to high and medium impact BES Cyber Systems and their associated EACMS and PACS.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
CIP-013-2 R1, Part 1.2.6 requires one or more processes used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the coordination of controls for vendor-initiated (i) remote access, and (ii) system-to-system remote access. This language provides the two basic types of vendor remote access; however, it lacks the detail provided in CIP-005-7 R3, Parts 3.1 and 3.2, which may be required to effectively assess risk. Further, as discussed in the previous comments, the use of the term "vendor-initiated" is troubling because it should not matter whether the vendor or the entity initiates the connection. By considering only vendor-initiated connections, the language omits some vendor remote access connections, and therefore does not meet the security objective of the Requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State does not agree with the changes; we believe the CIP-013-1 language is more clear and comprehensive.

The previous CIP-013-1 wording

• “Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)”

is more clear and more comprehensive than the proposed CIP-013-2 wording

• “Coordination of controls for vendor-initiated (i) remote access, and (ii) system-to-system remote access.”

CIP-013-2’s “Coordination of controls for vendor-initiated … system-to-system remote access” seems to exclude system-to-system remote access that’s internally-initiated, where a system inside the ESP automatically creates a remote access session with a vendor’s system in the vendor’s network.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the SDT’s summary response under question 4.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders’ time on this

endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with

trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods. 2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions. 3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard. 4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.	
Erick Barrios - New York Power Authority - 6	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	

Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE agrees with clarifying that all types of vendor-initiated remote access needs to be considered. Texas RE recommends that the term "vendor" be defined in the NERC Glossary. Although it is defined in the Supplemental Material, that material is not part of the standard and is not enforceable. There is still confusion on who and what is a vendor.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment	
EEI supports the notion that all vendor-initiated remote access should be considered.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
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	
EEI supports the notion that all vendor-initiated remote access should be considered.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	

Evergy (Westar Energy and Kanas City Power & Light Co.) supports the position that all vendor-initiated remote access needs to be considered.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree with this revision that clarifies vendor-initiated remote access controls in supply chain risk management plans and processes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the reconstructed the wording clarifies that all types of vendor-initiated remote access needs to be considered.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
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	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
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	
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	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	

ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	

Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing an increase from 12 to 18 month implementation plan in response to industry comment. Do you agree this strikes a balance between appropriate risk mitigation and giving the industry time to implement changes?

Thank you for your comment. Based on the items listed below. The SDT determined that 18 months is sufficient. The SDT expanded the implementation time to 18 months based on the following criteria:

- EACMS and PACS represents a significant expansion in scope for both hardware and software that may undergo planned procurement.
- While CIP-013-2 does not require the Responsible Entity to renegotiate or abrogate existing contracts there is a recognition that (the large number of vendors and their contracts that are currently in place may need to be modified and renegotiated to cover any new existing equipment and systems that would need to be put in place.
- Vendors are possibly placed in several regions and jurisdictions and would take more time to consolidate the same policies and procedures across the entity.

In addition to the above, some entities expressed the consideration of budget cycles due to technological upgrades needed for the implementation along with the budgeting and planning efforts within most entities occur annually with the planning and finalization occurring a year in advance. Those technology upgrades may include but not be limited to:

- Implementing a Governance, Risk, and Compliance (GRC) solution if not already deployed within their organization.
- A Third Part Risk Management (TPRM) solution in concert with the entities' Supply Chain Management.

An 18-month implementation plan would allow organizations to address any change management, possible contract revisions, vendor additions, budget cycles, and policy modifications to be put in place in a timely manner.

Regarding the comments around COVID-19, the SDT believes that 18 months provides adequate time to implement the revisions as well as accommodate issues resulting from the pandemic response in accordance with the NERC-issued guidelines that entities may leverage if COVID-19 materially impacts any ability to comply with periodic requirements or future enforceable standards.

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	
Comment	
We think 24 months better supports the process we have at a small utility with minimal IT resources.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Due to the Covid-19 impacts to industry, we suggest considering a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response:

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline

within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

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

Due to the Covid-19 impacts to industry, the virtualization standards under development, and supply chain standards implementation overall, it is recommended to consider a 24-month implementation plan.

Likes 0	

Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
It appears that the basis for the originally proposed 12-month implementation centers on an assumption that EACMS and PACS vendors are the same for high impact and medium impact BES Cyber Systems. This supposition would make it appear that it is a straightforward expansion of existing Supply Chain programs to EACMS and PACS. This is not true in all cases. Notably, the high impact (e.g. control center) and medium impact (e.g. substation) environments are very different. CEHE believes that such a difference justifies a longer implementation period. CEHE suggests that 18 months is not enough and proposes a 24-month implementation plan instead.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	

Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
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. Please see the SDT response at the beginning of question 5.	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
These changes are adjustments to existing standards, and 12 months is plenty of time to implement the changes.	
Likes 0	
Dislikes 0	
Response:	

Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Due to the on-going Covid-19 impacts and delay of initial supply chain standards implementation, it is recommended to consider a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Wayne Guttormson - SaskPower - 1	

Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Due to the development of the virtualization standards, and supply chain standards implementation overall, we recommended to consider a 24 month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
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	
Due to the Covid-19 impacts to industry, the virtualization standards under development, and supply chain standards implementation overall, it is recommended to consider a 24 month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

MidAmerican appreciates the proposed increase to the implementation plan. However, we recommend consideration of a 24-month implementation plan in order to provide time for NERC to coordinate ongoing efforts of other SDTs that may also impact the supply chain standards.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican appreciates the proposed increase to the implementation plan. However, we recommend consideration of a 24-month implementation plan in order to provide time for NERC to coordinate ongoing efforts of other SDTs that may also impact the supply chain standards.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	No
Document Name	
Comment	

In order to properly evaluate and fund required changes a longer implementation period of 24 months is required. This is necessary to obtain possible funding and process changes that would be necessary.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with a longer implementation plan window.	
Likes 0	

Dislikes 0	
Response:	
Thank you for your support.	
Erick Barrios - New York Power Authority - 6	
Answer	Yes
Document Name	
Comment	
We agree with the SDT proposal	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response:	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports the 18 month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
NV Energy agrees that the the extension in implementation timeline is acceptable; however, with the expectation of revisions to the CIP Standards through Project 2016-02, and the concurrent work required to implement these future changes, NV Energy would request that NERC look to further extend this implementation timeline to ensure Entities have enough time to implement the concurrent revisions.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. The project 2016-02 is a separate project and will have a new implementation plan allowing entities to adjust accordingly once that project is completed. Please see the SDT response at the beginning of question 4 as to why 18 months is a sufficient timeframe for the Project 2019-03 Implementation plan.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the proposed 18-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes

Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) supports the 18-month implementation plan and the extended implementation period appropriate when considering the expanded applicability of the Standards.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Although 24 months would be more appropriate, GTC/GSOC appreciate the SDT's consideration of previous comments.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
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	

EEI supports the 18-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO agrees with the increase of the implementation period from 12 moths to 18 months. IESO would prefer 24 months to take budget cycles into account. Although the we acknowledges that EACMS and/or PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to EACMS and or PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years to allow for the processes and controls to mature and to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment	
EEI supports the 18-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Although 24 months would be more appropriate, GSOC and GTC appreciates the SDT's consideration of previous comments.	
Likes 0	
Dislikes 0	
Response.	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	Yes
Document Name	
Comment	

The IRC SRC supports the SDT changes to extend the implementation timeframe from 12 to 18 months. In addition, the IRC SRC requests the SDT consider an additional extension of the implementation timeframe to 24 months to accommodate budget cycles.

Although the IRC SRC acknowledges that EACMS and/or PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. 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.

At this time, it is unknown whether the existing supply chain requirements will have a tangible improvement in supply chain security, so the IRC SRC recommends any expansion in the scope of requirements be deferred until more is known.

Likes 0	
Dislikes 0	

Response:

Thank you for your comment. Please see the SDT response at the beginning of question 5.

Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

CAISO is supporting the IRC SRC Comments as follows:

The IRC SRC supports the SDT changes to extend the implementation timeframe from 12 to 18 months. In addition, the IRC SRC requests the SDT consider an additional extension of the implementation timeframe to 24 months to accommodate budget cycles.

Although the IRC SRC acknowledges that EACMS and/or PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. 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. At this time, it is unknown whether the existing supply chain requirements will have a tangible improvement in supply chain security, so the IRC SRC recommends any expansion in the scope of requirements be deferred until more is known.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Randy Cleland - GridLiance Holdco, LP - 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	
Anthony Jablonski - ReliabilityFirst - 10	
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	
Steven Rueckert - Western Electricity Coordinating Council - 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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 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	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
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	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
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	
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	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 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	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,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	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	

Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	

6. 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. 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 comment. 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.

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP would first like to see the definitions that are outlined in CIP-005 and CIP-013 with more clarity and a better definition for each.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

CAISO is supporting the IRC SRC Comments as follows:

Although the IRC SRC acknowledges that EACMS and PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. 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. At that time, the IRC SRC also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.

While the IRC SRC believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory requirements should not be applied to additional Cyber Assets. When a regulatory compliance requirement is expanded to include additional assets in the enterprise, it increases 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. Therefore, the IRC SRC opposes adding EACMS or PACS to the supply chain requirement as this requirement has not yet proven to be effective as it stands.

Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	No
Document Name	
Comment	

In order to properly evaluate and fund required changes a longer implementation period of 24 months is required. This is necessary to obtain possible funding and process changes that would be necessary.

Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	No
Document Name	
Comment	
Although the IRC SRC acknowledges that EACMS and PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. 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. At that time, the IRC SRC also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard. While the IRC SRC believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory requirements should not be applied to additional Cyber Assets. When a regulatory compliance requirement is expanded to include additional assets in the enterprise, it increases 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. Therefore, the IRC SRC opposes adding EACMS or PACS to the supply chain requirement as this requirement has not yet proven to be effective as it stands.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	

Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
It's difficult to determine the cost since CIP-013 is not effective and no studies have been conducted to determine the cost to implement across the industry. Including PACS and EACMS adds another layer to consider once the BCS' Supply Chain Risk Management requirements are implemented. The scope continues to expand without consideration to the industry as a whole to first achieve the risk mitigations for the initial standards and without studies to determine the effectiveness of the Supply Chain Risk Management standards for BCS'. Unless small entities contract with 3rd parties for the vendor risk assessments required, what is their alternative since vendors usually do not respond to their cyber security questionnaires. Suggest determining the effectiveness of the first CIP-013 standards before adding more systems to the requirements and potentially adding additional costs.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
While GSOC and GTC acknowledges the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.	
Likes 0	

Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
The burden on the industry will increase with expanding the scope of these requirements to include EACMS and PACS. The cost of this burden cannot be credibly estimated at this time. Costs and benefits need to be considered for both the industry and vendors.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
The burden on the industry will increase with expanding the scope of these requirements to include EACMS and PACS. The cost of this burden cannot be credibly estimated at this time. Costs and benefits need to be considered for both the industry and vendors.	
Likes 0	
Dislikes 0	
Response:	

Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
While GTC/GSOC acknowledge the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	

Answer	No
Document Name	
Comment	
The larger inclusion of Cyber Assets (EACMS and PACS) increases the scope and burden on industry. The cost of CIP-013 compliance is currently unknown as this is a new standard. This potentially adds an additional set of Vendors/Supplier's that provide equipment, software, or service. Therefore, currently providing any credible cost or benefit information is premature. External increased costs imposed on industry by our vendors is also an unknown variance that cannot be predicted at this time.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No

Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
We do not agree the modifications are cost effective at this time. This is based on the current effort to implement CIP-013-1, CIP-005-6, and CIP-010-3 has not been completed and therefore a full understanding of the current costs is not known..	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	

The current language in the standard intentionally creates different expectations for vendor remote access versus internal staff remote access. As this subjects the entity to potentially multiple frameworks for the same activity, it inherently creates an inefficiency to the process that could be easily eliminated. Furthermore, the current measures in CIP-005 Part 3.1 introduce process activities that go beyond the stated requirements (i.e. monitoring remote access activity), potentially leading entities to implement more costly approaches to meet the standard requirements.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
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 that EACMS and PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to EACMS and PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years to allow for the processes and controls to mature and to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors to ensure they are implemented in the most cost-effective manner. At that time, the ISO-NE also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
The larger inclusion of Cyber Assets (EACMS and PACS) increases the scope and burden on industry. The cost of CIP-013 compliance is currently unknown as this is a new standard. This potentially adds an additional set of Vendors/Supplier's that provide equipment, software, or service. Therefore, currently providing any credible cost or benefit information is premature. External increased costs imposed on industry by our vendors is also an unknown variance that cannot be predicted at this time	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
The ambiguity around what "access" is, what "remote" is, and what "vendor" is in combination with the broad spectrum of interpretations by stringing these terms together creates a level of confusion that reduces cost effectiveness and efficiency. Additionally, the continued absence of a provision for emergencies in CIP-013 R1 forces a Registered Entity to choose between compliance and reliability, and that very condition puts reliability at risk and creates costly undue compliance overhead. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is not cost effective for industry to allocate our limited resources to unnecessary compliance overhead when doing the right thing in crisis. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18,	

2020 clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively manage the "knowns" and effectively mitigate the risk of the "unknowns". The simple inclusion of something like "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances".	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6. In addition, the CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Additional costs will be driven to add those new EACMS and PACS assets to supply chain overview.	
Likes 0	
Dislikes 0	
Response:	

Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Depending upon how an entity implements their initial Supply Chain Standards program, the proposed changes to CIP-005, CIP-010 and CIP-013 could result in significant impacts to an entity's program and may not be as simple as merely adding a few additional systems. For these entities, they may need to develop and implement a different process for EACMS and PACS systems.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
To minimize churn among standard versions, 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 SDT response at the beginning of question 6.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments Continual changes to standards and parts, even the slightest language and word changes cost budgetary dollars to review, comprehend, perform impact analysis, implement, test, and meet at audit. The ambiguity around what “access” is, what “remote” is, and what “vendor” is in combination with the broad spectrum of interpretations by stringing these terms together creates a level of confusion that	

reduces cost-effectiveness and efficiency. In the past, Standards Drafting Teams appear to work in silos from each other resulting in bleed over language which is similar or the same result.

Additionally, the continued absence of a provision for emergencies in CIP-013 R1 forces a Registered Entity to choose between compliance and reliability, and that very condition puts reliability at risk and creates costly undue compliance overhead. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is not cost-effective for industry to allocate our limited resources to unnecessary compliance overhead when doing the right thing in crisis. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020, clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective-based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively manage the "knowns" and effectively mitigate the risk of the "unknowns". The simple inclusion of something like "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances".

Likes 0	
Dislikes 0	

Response:

Thank you for your comment. Please see the SDT response at the beginning of question 6. In addition, CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.

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

Answer	No
Document Name	

Comment

Inclusion of EACMS and PACS to CIP-005 R3 Part 3.1 will require significant investment to isolate these Boundary Assets to be able to monitor for and terminate vendor remote access sessions. This is a substantial change to definition of EACMS and PACS and likely will bring additional assets into scope by requiring entities to define the new boundaries and cyber security isolation methods that had previously not been required.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State recommends EACMS be separated into EACS and EAMS. Not separating the concept of an EACMS into an EACS and EAMS creates lower BES security, as monitoring of industrial control system networks is not being integrated with monitoring of business networks, sensor networks, and other networks. A particular pain point is that EACMS requirements prevent outsourcing 24x7 network monitoring that includes systems or networks in CIP scope. The financial and human resources needed to apply EACMS compliance levels to monitoring (not controlling) are unnecessary.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Dennis Sismaet - Northern California Power Agency - 6	

Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response: 1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy does not agree the modifications are cost effective at this time. This is based on the current effort to implement CIP-013-1, CIP-005-6, and CIP-010-3 has not been completed and therefore a full understanding of the current costs is not known to establish a baseline with which to measure against. Duke Energy sees potential schedule and cost risks in implementing yet to be defined tools in the required time period. Also, Duke Energy has yet to evaluate the impacts of defining and implementing EACMS and PACS related controls to meet this requirement.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
We do not feel that the level of administration and additional work is not cost effective for small organizations with limited resources. We recommend that exceptions are made for smaller entities that are more limited in their ability to get competative bids, and services to meet the intent of the FERC directives.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees that the FERC directives can be executed in a cost-effective manner. There will be an undue cost and burden initially to conduct business another way by adding EACMS and PACS to CIP-005 R3.1 and R3.2. Other costs will include providing new technology if not already present to track, store, and recall the data addressing the assessments provided by CIP vendors.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	

No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
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	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
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	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10	
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	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	

ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) does not have a position nor comments in response to Question 6.	

Likes 0	
Dislikes 0	
Response	
Thank you.	
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	
Document Name	
Comment	

The addition of EACMs and PACs to the CIP-005 requirement 3 adds significant compliance efforts and costs to responsible entities. Entities that use vendors to assist in access monitoring, electronic or physical, for monitoring and threat hunting is a good thing. The more eyes on potential nefarious activity provides for a safer and more reliable grid.

Efforts like this sound good but do nothing to add to the cyber security of the grid.

Using the measure cited in part 3.1 as an example "Methods for monitoring activity (e.g. connection tables or **rule hit counters in a firewall**, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions" are now standard in most firewalls and can be provided as a print out for evidence. This however does nothing to secure the grid. The standards should address alerting on and actions taken on a unrecognized connections by an outside source. This would be more in line with providing cyber security, automated processes that transmit logs to SEIMS monitored by outside vendors is better for security. These types of issues should be addressed in CIP-013 requirement 1 already addresses connections inbound and outbound to assets.

Continual changes to standards and parts, even the slightest language and word changes cost budgetary dollars to review, comprehend, perform impact analysis, implement, test and meet at audit. The ambiguity around what “access” is, what “remote” is, and what “vendor” is in combination with the broad spectrum of interpretations by stringing these terms together creates a level of confusion that reduces cost effectiveness and efficiency. In the past, Standards Drafting Teams appear to work in silos from each other resulting in bleed over language which is similar or the same result.

Additionally, the continued absence of a provision for emergencies in CIP-013 R1 forces a Registered Entity to choose between compliance and reliability, and that very condition puts reliability at risk and creates costly undue compliance overhead. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is not cost effective for industry to allocate our limited resources to unnecessary compliance overhead when doing the right thing in crisis. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively manage the "knowns" and effectively mitigate the risk of the "unknowns". The simple inclusion of something like "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances".	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6. In addition, CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
No comment	

Likes 0	
Dislikes 0	
Response	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	

7. Provide any additional comments for the standard drafting team to consider, if desired.	
Calvin Wheatley - Wabash Valley Power Association - 1,3	
Answer	
Document Name	
Comment	
Wabash Valley Power Alliance supports the comments submitted by NRECA. We individually comment that the low impact category has highly varied risk levels. This is especially true when a single access point controls access to a large number of BES assets. It is essential to impose BES Reliability standard on those systems whose architecture has a potential broad scale affect on reliability, while not adding excessive burden and costs on systems that are architected to have a minimal effect on grid reliability. Appropriate risk assessment by the SDT to focus efforts on those systems that will have an affect on grid reliability should be included as a component of the SAR.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT was unable to locate NRECA comments. After reading the comments above, it appears this comment may be for a different standards project.	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending an inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provide a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed though the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent out for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline

within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	
Document Name	
Comment	
AZPS requests more information be provided regarding the rationale for leaving the "system-to-system remote access" and "Interactive Remote Access" language in the Measures section of CIP-005-7 R3.1 and R3.2, after removing the language from the requirements. AZPS notes that the Measures section for CIP-005-7 R3.2 still references disabling remote access versus terminating remote access sessions. AZPS recommends that the SDT revise the Measures to maintain consistency with the requirement language. Similarly, AZPS recommends revising the language in CIP-013-2 R1.2.6 to maintain consistency with the language in CIP-005-7 R3.1 and R3.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT's original intention was to mirror language found in the FERC Order. The SDT received several comments about confusion caused by these terms when relating them to EACMS and PACS. The SDT considered this unintended consequence, and to address industry concerns is proposing alternative language that no longer requires reference to these terms and undefined phrases. The SDT also considered feedback about consistency and has adjusted the measures to align with the proposed language of the draft.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	

Within 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. The CIP-005-7 Implementation Guide for R3 uses the term "periodic" in every example of internal controls – with no definition or assistance regarding how long "periodic" is.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. PCAs are not within scope for this SAR.	
Erick Barrios - New York Power Authority - 6	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents. In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, "General Considerations for Requirement R2" should read "General Considerations for Requirement R3". The text indicates "The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls ". 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. Your request has been passed along to NERC staff for consideration. In addition, supporting documents are located on the project. In addition, the noted modifications to the CIP-013-2 technical rationale have been updated.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	

Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	

Support SDT consideration of formally defining "vendor" in the NERC Glossary of Terms. With the supply chain CIP-013-2, suggest inclusion of PACS peripherals (badge readers).

There are significant risks associated with PACS peripherals.

When contactless smart cards are implemented and deployed properly, they represent one of the most secure identification technologies available. However, some manufacturers, in an attempt to sell a 'universal' reader capable of reading almost any contactless smart card technology, actually disable the built-in security mechanisms. These readers, referred to as 'CSN readers', only read the card's serial number which, per ISO standards, is not be protected by any security. The ISO standard specifies use of the CSN for a process referred to as anti-collision, which is designed only to identify more than one distinct card in the field of the reader, and does not include security measures. An understanding of these details can allow a perpetrator to build a device to clone (or simulate) the CSN of a contactless smart card.

CSN refers to the unique card serial number of a contactless smart card. All contactless smart cards contain a CSN as required by the ISO specifications 14443and 15693. The CSN goes by many other names including UID (Unique ID), and CUID (Card Unique ID). It is important to note that the CSN can always be read without any security or authentication per ISO requirements.

Providers who seek to provide the lowest cost product, often choose not to pursue proper licensing of the security algorithms to minimize their costs. They also often fail to educate their customers on the compromise they are introducing into the customer's security solution. While the customer may benefit from a low price at install, the long term cost of a security compromise can be catastrophic. (Source - HID Global)

Emerging PACS technology includes IP Based Door Access and Entry Control Systems. This eliminates the need for a door controller. The built in intelligence system within the badge reader allows the access control decision to be made at the door controller in the event the network is down.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT considered feedback about defining the term "vendor" and decided not to create a formal glossary of terms definition to allow needed flexibility for each entity to document within their plan what constitutes a vendor. Instead,

the SDT has documented their intent regarding the use of this undefined term within the Technical Rationale for CIP-013-2; which reads, "The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators." Regarding PACS peripherals, the SDT's inclusion of PACS in CIP-013-2 does not modify nor superseded the NERC Glossary of Terms definition and exclusions for PACS which states, "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers." There is an appreciation that emerging technologies may change the manner within which certain technologies operate; however, due to the pervasive use of the term PACS, it is not within the scope of the 2019-03 SAR to modify this definition.

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

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

The changes proposed have little to do with Supply Chain. When considering Supply Chain and vendors and their remote access, the SDT must re-review the SAR and separate concepts with personnel and their authorizations from systems and their authorized purposes and capabilities. This can be achieved by minor changes in the following:

CIP-004-6 already includes controls for authorizing personnel and is the appropriate standard area to authorize vendors. Consider authorization and access of personnel (no matter employees, contractors, or vendors).

CIP-002 is a more appropriate choice for identifying and categorizing vendor systems that reside at an entity location. This allows an entity to use existing processes to identify vendor vs entity BCS and define and declare the purpose of the vendor system – i.e., providing vendor remote access – much as an entity identifies an EACMS or PACS purposes. This allows an entity to consider the capability and define what systems/cyber assets and software are authorized vs what they have not authorized (similar to how an entity authorizes people). CIP-005, CIP-007, and CIP-010 already address controls for configurations, accounts, and network/firewall rules) including identifying the protocols (RDP, SSH, etc..) ingress/egress to a BCS and a business justification in CIP-005. In this case, the justification would be "vendor remote access." These considerations use language and controls which separate and authorize people from authorizing systems and allows an entity to focus on defining the people, their authorizations and accounts (for vendors), and allows a focus on defining the purpose and function of a BCS, its configured apps and account privileges.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Standard Drafting Teams (SDTs) have been in communication and continue to be in communication. After the teams reviewed the proposed EACMS split by project 2016-02, it was determined that this split is outside the scope of all three CIP SDTs (Project 2016-02 (CIP Virtualization), 2019-02 (CIP BCSI), and 2019-03 (Supply Chain)). A SAR will be drafted and submitted for future consideration. Any modifications made by project 2016-02, will be made following the completion of the 2019-03 project.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDTs response to EEI.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDTs response to EEI.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
There are cases where the requirements would include “BES Cyber Systems, and their associated EACMS and PACS” as Applicable Systems (such as in CIP-010-4 Part 1.6, CIP-013-2 R1, R1.1, R1.2, R1.2.5). If associated PCAs are not included, the rest of the cyber assets within an	

Electronic Security Perimeter will be vulnerable. For example, PCA patches may be inadvertently loaded with Trojan Horses, malicious sniffers, etc., which may affect the rest of the devices in the network – including BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT appreciates the concerns raised and has not removed PCAs from the Applicable Systems of existing approved and future enforceable requirements; however, it is also not within the scope of the 2019-03 SAR to include PCAs in any new or modified requirements where PCAs do not already exist. The absence of PCAs does not preclude an entity from implementing processes that go above and beyond the minimum requirements of the Standard, and entity's may choose based on risk to include PCAs within their program.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDTs response to Snohomish PUD.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	

Santee Cooper has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	
Document Name	
Comment	
Consistency across the three supply chain standards is of paramount importance. Please consider integrating consistent language into each standard, as applicable.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Thank you for your comment. The team reviewed to ensure language is consistent across the three Supply Chain standards. The SDT notes that while some words may be considered 'not consistent', it makes sense for the use within the appropriate requirement language.	
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	
Document Name	

Comment	
The clarification of vendor-initiated in CIP-005 R3 is valuable, but it doesn't solve the challenge of a contract employee (a vendor according to Supplemental Material sections of the Standards). A contract employee who initiates access to an applicable system remotely would be subject to these requirements, even if they are using Registered Entity owned and managed systems to initiate that access.	
Likes 0	
Dislikes 0	
Response	
The SDT considered feedback about defining the term "vendor" and decided not to create a formal glossary of terms definition to allow needed flexibility for each entity to document within their plan what constitutes a vendor, and believes there is sufficient detail within the Implementation Guidance and Technical Rationale for CIP-013-2 clarifying that it is up to the entity to define vendor. The SDT has documented their intent regarding the use of this undefined term within the Technical Rationale for CIP-013-2; which reads, "The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	

Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI.	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents. In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, "General Considerations for Requirement R2" should read "General Considerations for Requirement R3". The text indicates "The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls ". 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. Your request has been passed along to NERC staff for consideration. In addition, supporting documents are located on the project. In addition, the noted modifications to the CIP-013-2 technical rationale have been updated.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
No additional comments on this question.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	
Document Name	
Comment	
CHPD maintains that it does not agree with the inclusion of PACS in the scope of Project 2019-03. As stated in Cyber Security Supply Chain Risks Staff Report and Recommended Actions, "The potential risk of supply chain compromise described can be mitigated in part by	

controls, some of which are addressed it the CIP Reliability Standards while others can be addressed in entity policies and procedures … In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." (p. 14-15). CHPD agrees that PACS pose a lower risk to the BES than other classifications (BCA, EACMS, and PCA). PACS have no 15-minute BES impact and no access to BCS or ESP. CHPD believes that PACS should be excluded from Project 2019-03 for CIP-010 and CIP-013 due to their lower risk to the BES. CHPD instead recommends a best practice approach and adequate cyber security controls be applied to PACS for the same justification as to why they were applied to PCAs in the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019, p. 21-22) CHPD requests coordination between Project 2016-02 and 2019-03 as changes of the EACMS classification continues to be developed.

Likes 0	
Dislikes 0	

Response
The SDT appreciates the thorough nature of comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS: 1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.", 2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and 3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks". In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to

protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.
The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.
Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."
While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.
Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through
a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.
The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore, the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.

Lastly, The SDT must include EACMS in CIP-005-7 to meet FERC directives. In Order No. 850 the "supply chain risk management Reliability Standards" is a term that collectively refers to CIP-013-1, CIP-005-6, and CIP-010-3. Therefore, any directives which pertain to the supply

chain risk management Reliability Standards pertain to the entire set of above listed Standards. Specifically, paragraph 1 describes the term at the outset of the Order No. 850:

"Pursuant to section 215(d)(2) of the Federal Power Act (FPA), the Commission approves supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)."

Paragraph 5 of Order No. 850 is the first time instance of the directive:

"To address this gap, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…"

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

The continued absence of a provision for emergencies in CIP-013 R1 creates a condition where a Registered Entity must choose between compliance and reliability, and that very condition puts reliability at risk. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances by their very nature are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant for a Requirement that was intended to be future-looking and not operational. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively plan for the "knowns" while effectively mitigating the risk of the "unknowns" without a violation. The simple inclusion of

something like "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances". ATC believes it was the original SDT's intention for this to be a future-looking planning standard instead of a real-time/near real-time operating horizon standard, and does not believe it was the original drafting team's intention to penalize Registered Entities when performing emergency procurements based on operational emergencies, yet the FAQ and the emerging guidance from our regulators would interpret this as a violation. If CIP Exceptional Circumstances was not considered, or omitted, by the original SDT due to past understanding that such emergencies are "unplanned" and therefore not subject to CIP-013-1, and the current SDT is aware of this unintended consequence and oversight, then the current SDT should be permitted to make that clarifying change under the existing SAR. A provision like this benefits reliability because now we are all thinking about this as a potentiality and could be better prepared to respond in crisis without having to choose between compliance and reliability. ATC appreciates the consideration.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI.	

Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	
Document Name	
Comment	

CHPD maintains that it does not agree with the inclusion of PACS in the scope of Project 2019-03. As stated in Cyber Security Supply Chain Risks Staff Report and Recommended Actions, "The potential risk of supply chain compromise described can be mitigated in part by controls, some of which are addressed it the CIP Reliability Standards while others can be addressed in entity policies and procedures … In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." (p. 14-15). CHPD agrees that PACS pose a lower risk to the BES than other classifications (BCA, EACMS, and PCA). PACS have no 15-minute BES impact and no access to BCS or ESP. CHPD believes that PACS should be excluded from Project 2019-03 for CIP-010 and CIP-013 due to their lower risk to the BES. CHPD instead recommends a best practice approach and adequate cyber security controls be applied to PACS for the same justification as to why they were applied to PCAs in the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019, p. 21-22)

CHPD requests coordination between Project 2016-02 and 2019-03 as changes of the EACMS classification continues to be developed.

Likes 0	
Dislikes 0	

Response

The SDT appreciates the thorough nature of comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:
1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through

a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore,

the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.
The SDT must include EACMS in CIP-005-7 to meet FERC directives. In Order No. 850 the "supply chain risk management Reliability Standards" is a term that collectively refers to CIP-013-1, CIP-005-6, and CIP-010-3. Therefore, any directives which pertain to the supply chain risk management Reliability Standards pertain to the entire set of above listed Standards. Specifically, paragraph 1 describes the term at the outset of the Order No. 850:

"Pursuant to section 215(d)(2) of the Federal Power Act (FPA), the Commission approves supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)."

Paragraph 5 of Order No. 850 is the first time instance of the directive:

"To address this gap, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…"

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

Answer	
Document Name	

Comment

Southern would like, as with EEI, for the SDT to more clearly define how vendor remote access is to be addressed when a staff augmented contractor is essential to the reliable operations to the BES. Proposed Reliability Standard CIP-005-7 does not provide a mechanism that exempts vendors who are providing essential contract services that include regular access to High and Medium Impact BES Cyber Systems, and associated EACMS, PACS and PCA.

Consider a proposal to modify the SAR to remove EACMS from the scope of CIP-005.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to EEI.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	
Comment	
We appreciate the SDT efforts. Cyber Security is an ever changing issue and the Standard development process is just too slow for specifics. We believe entities should be required to regularly evaluate the risks and develop their own risk-based mehods of protection. This approach would allow entities to concentrate more on protecting the BES and less on complying with specific requirements that may or may not be adequate or cost effective. This approach would likely result in fewer findings of non-compliance and more recommendations for improvement, but provide more effective Critical Infrastructure Protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed CIP-013 and believes the requirements are written in a manner that allows this type of flexibility.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	

Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Your request has been passed along to NERC staff for consideration.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Your request has been passed along to NERC staff for consideration.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to MRO NSRF.	
Wayne Guttormson - SaskPower - 1	
Answer	
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to MRO NSRF.	
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	
Document Name	
Comment	
These changes proposed have little to do with Supply Chain. When considering Supply Chain and vendors and their remote access, the SDT may must re-review the SAR and separate concepts with personnel and their authorizations from systems and their authorized purposes and capabilities. This can be achieved by minor changes in the following:	

CIP-004-6 already includes controls for authorizing personnel and is the appropriate standard area to authorize vendors. Consider authorization and access of personnel (no matter employees, contractors or vendors).

CIP-002 is a more appropriate choice for identifying and categorizing vendor systems which reside at an entity location. This allows an entity to use existing processes to identify vendor vs entity BCS and define and declare the purpose of the vendor system – i.e., providing vendor remote access – much as an entity identifies an EACMS or PACS purposes. This allows an entity to consider the capability and define what systems/cyber assets and software are authorized vs what they have not authorized (similar to how an entity authorizes people).

CIP-005, CIP-007 and CIP-010 already address controls for configurations, accounts and network/firewall rules) including identifying the protocols (RDP, SSH, etc..) ingress/egress to a BCS and a business justification in CIP-005. In this case the justification would be "vendor remote access."

These considerations use language and controls which separate and authorize people from authorizing systems and allows an entity to focus on defining the people, their authorizations and accounts (for vendors), and allows a focus on defining the purpose and function of a BCS, its configured apps and account privileges.

Secondly, the continued absence of a provision for emergencies in CIP-013 R1 creates a condition where a Registered Entity must choose between compliance and reliability, and that very condition puts reliability at risk. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances by their very nature are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant for a Requirement that was intended to be future-looking and not operational.

NERC should implement language to fix this so we can effectively plan for the "knowns" while effectively mitigating the risk of the "unknowns" without a violation. The simple inclusion for example of "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances". It was the original SDT's intention for this to be a future-looking planning standard team instead of a real-time/near real-time operating horizon standard, and was not NERC nor the original drafting team's intention to penalize Registered Entities when performing emergency procurements based on operational emergencies, yet the FAQ and the emerging guidance from our regulators would interpret this as a violation. If CIP Exceptional Circumstances was not considered, or omitted, by the original SDT due to past understanding that such emergencies are "unplanned" and therefore not subject to CIP-013-1, and the current SDT is aware of this unintended consequence and oversight, then the current SDT should be permitted to make that clarifying change under the existing SAR. A provision like this benefits reliability because now we are all thinking about this as a potentiality and could be better prepared to respond in crisis without having to choose between compliance and reliability. ATC appreciates the consideration.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. Please see the SDT's response to MRO's comments.

Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	
Document Name	

Comment
N/A

Likes 0	
Dislikes 0	

Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) incorporate by reference the Edison Electric Institute's response to Question 7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI Q7.	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	
Document Name	
Comment	
Puget Sound Energy supporte the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI.	

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	
Request that NERC notifies the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that the industry wants to provide feedback on the corrected, up-to-date documents. In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, "General Considerations for Requirement R2" should read "General Considerations for Requirement R3". The text indicates "The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cybersecurity risk management controls ". R2 requires the responsible entity to implement its supply chain cybersecurity 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. Your request has been passed along to NERC staff for consideration. In addition, supporting documents are located on the project. In addition, the noted modifications to the CIP-013-2 technical rationale have been updated.	
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	
EEI asks the SDT to more clearly define how vendor remote access is to be addressed when the service vendor is essential to the reliable operation the BES. Proposed Reliability Standard CIP-005-7 does not provide a mechanism that exempts vendors who are providing essential contract services such as security access monitoring, logging and control through remote access to High and Medium Impact BES	

Cyber Systems, and associated EACMS, PACS and PCA. Presently, approved service vendors who require access to these systems are required to undergo personnel risk assessments through CIP-004-6, just as internal staff that needs similar access to these systems. Entity use of these services is often necessary to augment internal expertise or tools to perform these highly specialized duties necessary for the reliable operation of the BES or when project based work requires temporary vendor service providers to work on BES related equipment or software. The current draft of CIP-005-7, Requirement R3 does not distinguish between those service vendors who are properly vetted and those who are not authorized for remote access. For this reason, we are concerned that without an exemption for those service vendors that have already been vetted through the asset owner's CIP-004-6 process, many registered entities who safely and effectively use these services could be negatively impacted by the proposed Reliability Standard modifications. Among the services that could be impacted include the use of very specialized IT services needed to manage EACMS for BES Cyber Systems. To address this concern, EEI asks the SDT to consider scenarios where registered entities may use service vendors that would require vendor initiated remote access to EACMS for the purpose of enhancing or maintaining BES reliability and security.	
Likes 0	
Dislikes 0	
Response	
Thanks for your comment. Please see the SDT's response to EEI.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Your request has been passed along to NERC staff for consideration.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI asks the SDT to more clearly define how vendor remote access is to be addressed when the service vendor is essential to the reliable operation of the BES. Proposed Reliability Standard CIP-005-7 does not provide a mechanism that exempts vendors who are providing essential contract services such as security access monitoring, logging and control through remote access to High and Medium Impact BES Cyber Systems, and associated EACMS, PACS and PCA. Presently, approved service vendors who require access to these systems are required to undergo personnel risk assessments through CIP-004-6, just as internal staff that needs similar access to these systems. Entity use of these services is often necessary to augment internal expertise or tools to perform these highly specialized duties necessary for the reliable operation of the BES or when project based work requires temporary vendor service providers to work on BES related equipment or software. The current draft of CIP-005-7, Requirement R3 does not distinguish between those service vendors who are properly vetted and those who are not authorized for remote access. For this reason, we are concerned that without an exemption for those service vendors that have already been vetted through the asset owner's CIP-004-6 process, many registered entities who safely and effectively use these services could be negatively impacted by the proposed Reliability Standard modifications. Among the services that could be impacted include the use of very specialized IT services needed to manage EACMS for BES Cyber Systems. To address this concern, EEI asks the SDT to consider scenarios where registered entities may use service vendors that would require vendor initiated remote access to EACMS for the purpose of enhancing or maintaining BES reliability and security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Modifications to CIP-004 are out of the scope of the 2019-03 SAR. The SDT considered this concern and determined there is sufficient detail within the Implementation Guidance and Technical Rationale for CIP-013-2 clarifying that it is up to the entity to define vendor. The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations	

with whom the registered entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators." It is the SDT's intention for vendor to exclude staff augmentation or contracted resources that are an extension of the entity's employ and payroll.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	
MidAmerican supports EEI comments. MidAmerican also requests the standard drafting team consider adding language regarding CIP Exceptional Circumstances or other provisions for emergency procurements. The absence of such language could result in a Registered Entity having to choose between compliance and reliability in an emergency situation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI. In addition, CEC language is not within the team's scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	

Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
MidAmerican supports EEI comments. MidAmerican also requests the standard drafting team consider adding language regarding CIP Exceptional Circumstances or other provisions for emergency procurements. The absence of such language could result in a Registered Entity having to choose between compliance and reliability in an emergency situation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI. In addition, CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
GSOC and GTC notes that the replacement of the term "determine" with the term "detect" in CIP-005-7, R2.4 (now 3.1) creates significant technical issues and may be infeasible. More specifically, the revision to the term "detect" pre-supposes a technical method to automatically delineate or differentiate vendor–initiated sessions from other active remote access sessions, which may be technically infeasible. In the previous version of the Guidelines and Technical Basis, a method to identify all types of remote access and an ability to	

terminate vendor sessions was considered appropriate. This distinction is important because methods for identifying active remote access sessions may be able to identify active sessions, but may not be able to differentiate those sessions that are vendor-initiated. Accordingly, once active sessions are identified, human or manual intervention may be necessary to hone in on those sessions that are vendor-initiated, e.g., through use of dedicated vendor identification numbers or access names. For these reasons, GSOC and GTC recommends that the SDT revert the proposed revisions to use the term "determine."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The terminology and conceptual change to a 3 part requirement: "Detect/Terminate/Disable". The word "Determine" is unusual usage and not aligned with typical cyber security terminology. The reason for a separate requirement in our proposed R3.3 is simple; terminating existing sessions does not prevent an attacker from spawning new sessions, and it is very easy to automate such requests. The requirement to "disable active vendor remote access" is crippled by the word "active" because it does not clearly express a need to disable future sessions which are by definition not "active". Combining the two requirements is parsimonious of words to the point of obscuring the objective. Without a means of denying new sessions, whether granularly or globally, an entity could find themselves playing "whack-a-mole" with an adversary and never able to manually keep it with automated requests. An example of granular control might be disabling a specific vendor's remote access account, blocking requests from a specific IP address or range, or changing an authentication token or password for a particular user account's remote access. This could be an absolute block or a suspension on new sessions for a timed period. For a global option, examples include simply denying all remote access attempts via change to a global VPN policy, firewall rule, etc. This is the proverbial "take a fire axe to the Internet connection" option.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	
Document Name	
Comment	
CPS Energy appreciates the standards drafting team efforts and supports mitigating risks to the BES in a cost effective manner across industry.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We would like to thank the SDT for allowing us to comment on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
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 the SDT's response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to NPCC RSCC.	

End of Report