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
Comment Period Start Date:	1/27/2020
Comment Period End Date:	3/11/2020
Associated Ballot:	2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 IN 1 ST

There were 66 sets of responses, including comments from approximately 137 different people from approximately 96 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 added EACMS, with the currently approved definition as explained in the above Background section, to CIP-005, CIP-010 and CIP-013 where the SDT believed is consistent with the FERC Order. Do you agree with FERC's justification of adding EACMS, FERC Order 850 P57? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT added PACS, with the currently approved definition as explained in the above Background section, to CIP-005-7, CIP-010-4 and CIP-013-2. Do you agree with adding PACS? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. Based on the addition of PACS to CIP-005 R2.4 and R2.5 and the lower risk they pose to the BES, the SDT has modified the associated VSL's. A violation of failing to have a method for determining OR disabling for PACS is listed as a Moderate VSL, and a violation of failing to have a method for determining AND disabling is listed as a High VSL. Do you agree with the modified VSLs? If you do not agree, please explain and provide your recommendation.

4. The SDT is proposing a 12 month implementation plan. Do you agree with the proposed timeframe? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

5. 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.

6. 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	Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISONE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Jennifer Brey	Arizona Electric Power Cooperative	1	WECC
					Joseph Smith	Prairie Power , Inc.	1,3	SERC
					Steven Myers	North Carolina EMC	3,4,5	SERC
					Shari Heino	Brazos Electric Power	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.		
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1	Meaghan Connell	5		PUD No. 1 of Chelan County	Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
of Chelan County					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
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	RSC	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Shivaz Chopra	New York Power Authority	5	NPCC
					Mike Forte	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
					Caroline Dupuis	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Laura McLeod	NB Power Corporation	5	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Randy MacDonald	NB Power Corporation	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
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 added EACMS, with the currently approved definition as explained in the above Background section, to CIP-005, CIP-010 and CIP-013 where the SDT believed is consistent with the FERC Order. Do you agree with FERC's justification of adding EACMS, FERC Order 850 P57? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
The risk focus should be limited to controls only, not monitoring.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NO. Changes to these Standards are not needed at all!	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Changes to these Standards are not needed at all!	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Changes to these standards are not needed at all.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO

Answer	No
Document Name	

Comment

We agree with the addition of EACMS (and PACS) to CIP-005-7 and CIP-013-2, but a close examination of the currently approved definition(s) of EACMS (and PACS) prevents them from being added to Medium Impact BES Cyber Systems in CIP-010-4 Requirement R1, Part 1.6 as proposed.

EACMS are currently defined as:

“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.”

EACMS are tied to ESPs. ESPs only exist with respect to Medium Impact BES Cyber Systems connected using a routable protocol. EACMS monitor and control the EAP on an ESP, so only Medium Impact BES Cyber Systems with External Routable Connectivity apply.

We understand that Applicable Systems cannot simply be changed to “Medium Impact BES Cyber Systems with External Routable Connectivity” because that would take Medium Impact BES Cyber Systems out of scope.

We recommend, for clarity and consistency among CIP standards:

Insert:

“Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS; and

2. PACS”

Between High Impact and Medium Impact Applicable Systems in CIP-010-4 Requirement R1, Part 1.6.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC and GTC respectfully reiterate the cooperative sector's comments in response to the Commission's Notice of Proposed Rulemaking regarding the dearth of reliability benefit associated with inclusion of those assets that provide only monitoring and logging functions and capabilities. Review of the proposed revisions, however, confirms that they meet the FERC directive set forth in Order 850. For the reasons cited in previous comments, GSOC and GTC continue to have reservations regarding the reliability benefit that the application of the CIP-013, CIP-005, and CIP-010 requirements to electronic access monitoring systems would contribute. Moreover, GSOC and GTC also have concerns regarding: (1) the synergies between this project and other standards development projects that are evaluating the current definition of EACMS and (2) the reconciliation of the implementation of the directive with findings presented by NERC Staff in the NERC Supply Chain report "*to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.*" GSOC and GTC respectfully suggest that the ERO Enterprise and the SDT consider interdependencies between these efforts and evaluate opportunities to better integrate them to ensure that future standards and definition modifications do not beget the need for cyclical, periodic revisions to reconcile each new set of revisions proposed by these different, but inter-dependent projects.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes there is the potential for the definitions and requirements to be in conflict with Project 2016-02, specifically where Project 2016-02 is working on definitions of EACMS vs EACS/EAMS to address different risk and security architecture in a virtualized environment. Project 2016-02 should be permitted to finish the work and have a planned implement date prior to another revision being implemented.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
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 you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.

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

Answer	No
Document Name	

Comment

PG&E agrees with the addition of EACMS but does not agree with the use of EACMS as currently defined in the “Applicable System Columns in Tables” section of the Standard. Including EACMS which provides “access control”, “monitoring”, and “alerting” capabilities extend what FERC indicated in Order 850 which indicated only “access control”. PG&E believes the risk of EACMS which “only” provides monitoring and alerting capabilities is not the same as those which provide “access control” and should be excluded from the Standard. PG&E does indicate if an EACMS provides access control while at the same time monitoring and/or alerting capabilities it should be covered by the Standard.

PG&E recommends the definition in the “Applicable System Columns in Tables” section be altered to indicate only those EACMS which provide “access control” and that EACMS that only provide monitoring and alerting be excluded. A Technical Rationale document could be created to clearly indicate what type of EACMS would be covered with examples to help clarify any confusion. A potential benefit in making the “Applicable Systems Column in Table” indicate EACMS with only “access control” is to the Project 2016-02 SDT working on the

separation of EACMS into Cyber Assets for "access control" (EACS) and monitoring/alerting (EAMS). A clear indication of "access control" in the Project 2019-03 modifications could make it easier for the Project 2016-02 SDT to make conforming changes to CIP-005, CIP-010, and CIP-013 once they are ready to complete the work on the EACMS separation.	
Likes 1	Central Hudson Gas &amp;amp; Electric Corp., 1, Pace Frank
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT	

considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.

In addition, the SDT agrees with the commenters’ statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the “Background” section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2, Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	

ISO-NE disagrees with adding EACMS and PACS to CIP-005. CIP-005 was intended for access to High and PCA systems. In fact, EACMs are derived from the CIP-005 requirements.

The CIP standards and requirements are structured to address security concerns based on the criticality and risk to the BES. EACMS and PACS do not incur the same security concerns and do not have the same criticality or risk to the BES; therefore, EACMS and especially PACS should not be treated the same as High or Medium Impact systems that have a direct correlation to the reliability of the BES. Additionally, the co-mingled definition of “access control and monitoring” inherently elevates systems with monitoring only capability to a high-water mark, adding the need to incorporate burdensome and costly controls to extremely low risk systems for little benefit.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

Although the CAISO acknowledges that EACMS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to EACMS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from audit experiences including findings and areas of concerns identified by the auditors. At that time the CAISO also proposes 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

The SDT thanks you for your comment, however, FERC order 850 has an implicit deadline of December 1, 2020.

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GSOC and GTC respectfully reiterate the cooperative sector's comments in response to the Commission's Notice of Proposed Rulemaking regarding the dearth of reliability benefit associated with inclusion of those assets that provide only monitoring and logging functions and capabilities. Review of the proposed revisions, however, confirms that they meet the FERC directive set forth in Order 850. For the reasons cited in previous comments, GSOC and GTC continue to have reservations regarding the reliability benefit that the application of the CIP-013, CIP-005, and CIP-010 requirements to electronic access monitoring systems would contribute. Moreover, GSOC and GTC also have concerns regarding: (1) the synergies between this project and other standards development projects that are evaluating the current definition of EACMS and (2) the reconciliation of the implementation of the directive with findings presented by NERC Staff in the NERC Supply Chain report "*to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.*" GSOC and GTC respectfully suggest that the ERO Enterprise and the SDT consider interdependencies between these efforts and evaluate opportunities to better integrate them to ensure that future standards and definition modifications do not beget the need for cyclical, periodic revisions to reconcile each new set of revisions proposed by these different, but inter-dependent projects.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	

Answer	No
Document Name	

Comment

Xcel Energy supports EEI comments on this question. In addition, Xcel Energy suggests adding the following language after EACMS in that applicability column of CIP-005-6 R2.4 and R2.5, CIP-010-4 and CIP-013-2 "***that perform the function of controlling electronic access**.*" Xcel Energy believes that this language would bring into scope all systems the perform access controls at an ESP, while excluding systems that only perform monitoring and or logging.

Making this change is supported by the Commission in Order 850 P55, where they state that "the standard drafting team that is formed in response to our present directive may determine…what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standard." The limitation of EACMS is also supported by NERC in the Cyber Security Supply Chain Risks Staff Report where they state in the Recommended Actions to Address the Risks section of CH2, P9 that "upon evaluation of the supply chain-related risks associated with EACMSs, particularly those posed by compromise of electronic access functions, NERC staff recommends that the Supply Chain Standards be modified to include EACMSs that perform electronic access control for high and medium BES Cyber Systems."

The addition of EACMS that only perform logging and monitoring access to the Supply Chain Standards, especially CIP-005-6 R2.4 and R2.5, would likely cause additional operational costs and significant admirative burden on systems that both FERC and NERC have indicated are not of equal risk to the BPS as those systems that are performing access controls to an ESP.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.

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, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	No
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
While we agree with the addition of EACMS to CIP-005, CIP-010 and CIP-013, we suggest that the SDT consider creating a new requirement, CIP-005-7 R3, and move Part 2.4 and Part 2.5 to this new requirement. We believe that this will help to alleviate any	

confusion that may exist surrounding EACMS and Intermediate Systems.While we agree with the addition of EACMS to CIP-005, CIP-010 and CIP-013, we suggest that the SDT consider creating a new requirement, CIP-005-7 R3, and move Part 2.4 and Part 2.5 to this new requirement. We believe that this will help to alleviate any confusion that may exist surrounding EACMS and Intermediate Systems.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:	

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

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

Answer	No
Document Name	
Comment	

Overall, Southern DOES NOT agree with the addition of EACMS as it has been proposed in these draft Standards as it does not align with the requirement from FERC Order 850. The SDT needs to address the scenario of terminating vendor remote access to the (EACMS) assets that are used to allow and prevent vendor remote access. In essence, if I must only allow vendor remote access through an authorized and authenticated session at an EACMS, and that EACMS is the asset I would use to prevent vendor remote access to a BCS, how then can I also prevent vendor remote access to that very asset that I use to terminate that remote access? This results in illogical loop. Also consider how to handle situations where a vendor is managing EACMS on behalf of the entity where disabling access to access controls seems causes that type of an illogical loop.

FERC has not ordered adding EACMS requirements to exactly the same requirements that apply to BCS as part of this Supply Chain initiative by merely changing the Applicable Systems column. There could be less restrictive requirements or new requirements based on risk that could apply to EACMS. We agree with the FERC Order that there should be additional requirements for those EACS assets that perform “access control” functions and not merely monitoring and logging functions. Given the absence of an attempt to modify the NERC defined term for EACMS to clarify the difference between EACS and EAMS, we do not agree with the addition of EACMS at this time as the current definition of EACMS assets to which these new requirements would apply is above and beyond the scope addressed in the FERC Order and the NERC Final Report.

For these reasons, keeping requirements applicable to EACMS in CIP-010 and CIP-013 addresses the FERC Order, however Southern believes the SDT should remove EACMS from CIP-005 R2.4 and R2.5 until such time that the EACMS definition can be modified and new definitions of applicable systems be added to properly scope these requirements, and the SDT can address the infinite loop issues addressed above.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide. The illogical

loop can be solved by removing access to that EACMS itself by whatever means access is granted. The requirements do not require an EACMS to provide access to other EACMS. Please reference the draft implementation guidance for an example.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Tampa Electric supports EEI comments which supports the addition of EACMS and agrees that modifications to the supply chain standards to address EACMS and specifically controls for ensuring reliability and security as stated in FERC Order 850 at P47 is appropriate. The Commission stated that "the standard drafting team that is formed in response to our present directive may determine…what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standard." (Order 850 at P55) We also note that in the NERC Cyber Security Supply Chain Risks Report dated May 17, 2019; it recommended only "revising the standard to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems." (Chapter 2, Overview, P7) Hence, the Commission has provided the Standards Drafting Team sufficient latitude, within FERC Order 850, to focus the scope of EACMS based on supporting analysis.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No

Document Name	
Comment	
CIP-005 is not currently applicable to EACMS and PACS, along with items such as Electronic Security Perimeters, Electronic Access Points, and Interactive Remote Access. The proposed changes to CIP-005 R2.4 and R2.5 bring Interactive Remote Access applicability to EACMS / PACS. There should be clarity and differentiation between Interactive Remote Access for BES Cyber Systems / Protected Cyber Assets and vendor remote access for EACMS / PACS. Interactive Remote Access has additional controls, such as multi-factor authentication. The proposed changes can cause confusion on the applicability of Interactive Remote Access and other CIP-005 controls to EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
While the addition of PACS and EACMS may appear to meet the spirit of the FERC Order, the addition of these two device types to CIP-005 R2 Parts 2.4 and 2.5 poses a challenge. Interactive Remote Access relies on the presence of an Electronic Security Perimeter or an Electronic Access Point, neither of which is a requirement that applies to PACS or EACMS. In its current form, the addition of PACS and EACMS to CIP-005 R2 Parts 2.4 & 2.5 would only apply to system-to-system vendor remote access, and not vendor interactive remote access. There is more work to be done to include the intended target of IRA when adding PACS and EAMCS to the applicability column. Suggest either update the definition of IRA or remove the capitalization from the IRA term in requirement language of CIP-005 R2 Parts 2.4 & 2.5.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and agrees that Electronic Security Perimeter (ESP) and Electronic Access Point (EAP) are part of the definition of Interactive Remote Access (IRA), however, ESP and EAP are only used in the definition to determine where access begins: "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)." Since a vendor remote access originates from a Cyber Assets that is outside an Entity's ESP and is not at a defined EAP, then any remote access meets the definition of IRA. The definition goes on to include places remote access may be initiated from "1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors or consultants."	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	

Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within: CIP-007-6: Requirement R2 Parts 2.1, 2.2, and 2.3, Requirement R3 Parts 3.1, 3.2, and 3.3, Requirement R4 Part 4.1, Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5	

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	

Support the MRO comments.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4, CIP-011-2: Requirement R1 Parts 1.1 and 1.2, Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with adding EACMS to the Supply Chain Standards as currently described above.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

OPG supports RSC comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree conceptually with including EACMS but need to assess the risk and implementation.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
We agree conceptually on the intent but we think that there is a need to better define the requirements. The added requirements are in the IRA section of CIP-005 R2, one could think that for accessing the EACMS an Intermediate system is required.	

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC respectfully reiterates the cooperative sector's comments in response to the Commission's Notice of Proposed Rulemaking regarding the dearth of reliability benefit associated with inclusion of those assets that provide only monitoring and logging functions and capabilities. Review of the proposed revisions, however, confirms that they meet the FERC directive set forth in Order 850. For the reasons cited in previous comments, MPC continues to have reservations regarding the reliability benefit that the application of the CIP-013, CIP-005, and CIP-010 requirements to electronic access monitoring systems would contribute. Moreover, MPC also has concerns regarding: (1) the synergies between this project and other standards development projects that are evaluating the current definition of EACMS and (2) the reconciliation of the implementation of the directive with findings presented by NERC Staff in the NERC Supply Chain report "*to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.*" MPC respectfully suggest that the ERO Enterprise and the SDT consider the codependent nature of these efforts and evaluate opportunities to better integrate them to ensure that future standards and definition modifications do not beget the need for cyclical, periodic revisions to reconcile each new set of revisions proposed by these different, but inter-dependent projects.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide. The 2019-03 team has consulted with the 2016-02 team and believe the work we had done within our FERC deadline and does not conflict or impact the other teams work.

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

Answer	Yes
Document Name	

Comment

EEI supports the addition of EACMS and agrees that modifications to the supply chain standards to address EACMS and specifically controls for ensuring reliability and security as stated in FERC Order 850 at P47 is appropriate. The Commission stated that “the standard drafting team that is formed in response to our present directive may determine…what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standard.” (Order 850 at P55) We also note that in the NERC Cyber Security Supply Chain Risks Report dated May 17, 2019; it recommended only “revising the standard to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.” (Chapter 2, Overview, P7) Hence, the Commission has provided the Standards Drafting Team sufficient latitude, within FERC Order 850, to focus the scope of EACMS based on supporting analysis.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC

Answer	Yes
Document Name	
Comment	
We agree conceptually with including EACMS but need to assess the risk and implementation. We agree conceptually on the intent but we think that there is a need to better define the requirements. The added requirements are in the IRA section of CIP-005 R2, one could think that for accessing the EACMS an Intermediate system is required.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 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	
Tim Womack - Puget Sound Energy, Inc. - 3	
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	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
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	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
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	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
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	
Jeff Icke - Colorado Springs Utilities - 5	
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	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT	

considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	

2. The SDT added PACS, with the currently approved definition as explained in the above Background section, to CIP-005-7, CIP-010-4 and CIP-013-2. Do you agree with adding PACS? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

SDT General Response to PACS Inclusion

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.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

MidAmerican agrees with MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Thank you for your comment.

At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “PACS, excluding those that provide only alerting and logging”, however, this change could introduce the requirement of maintaining “lists” of PACS and what functions they provide.

The SDT agrees with the commenters’ statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the “Background” section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
While the addition of PACS and EACMS may appear to meet the spirit of the FERC Order, the addition of these two device types to CIP-005 R2 Parts 2.4 and 2.5 poses a challenge. Interactive Remote Access relies on the presence of an Electronic Security Perimeter or an Electronic Access Point, neither of which is a requirement that applies to PACS or EACMS. In its current form, the addition of PACS and EACMS to CIP-005 R2 Parts 2.4 & 2.5 would only apply to system-to-system vendor remote access, and not vendor interactive remote access. There is more work to be done to include the intended target of IRA when adding PACS and EAMCS to the applicability column. Suggest either update the definition of IRA or remove the capitalization from the IRA term in requirement language of CIP-005 R2 Parts 2.4 & 2.5.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	

Answer	No
Document Name	
Comment	
CIP-005 is not currently applicable to EACMS and PACS, along with items such as Electronic Security Perimeters, Electronic Access Points, and Interactive Remote Access. The proposed changes to CIP-005 R2.4 and R2.5 bring Interactive Remote Access applicability to EACMS / PACS. There should be clarity and differentiation between Interactive Remote Access for BES Cyber Systems / Protected Cyber Assets and vendor remote access for EACMS / PACS. Interactive Remote Access has additional controls, such as multi-factor authentication. The proposed changes can cause confusion on the applicability of Interactive Remote Access and other CIP-005 controls to EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
We agree conceptually with including PACS but need to assess the risk and implementation. However, we expect a lower return on investment on PACS. There should be some awareness message on the change for CIP-010-4 R1.6 on third party or shared infrastructure. Was it intentional to not capitalize electronic access point in CIP-005 R2.5 bullet three of the measures?	

Another issue with the change to the applicability of PACS on page 6 of the redlined standard document for CIP-010-4. We question whether the exception should be added or maybe it needs to also include part 1.1. I'm not sure it makes sense to include additional devices in part 1.6 that are not included in 1.1 given that 1.6 must be followed only when there is a change to the baseline defined in 1.1.

Likes 0	
Dislikes 0	

Response

Thank you for your comment.

The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting. Those with shared infrastructure (co-located or jointly owned BES facilities) need to review and reevaluate their agreements based on new or revised requirements.

The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.

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 addition of PACS as it has been proposed in these draft Standards as it does not align with the requirement from FERC Order 850. The SDTs has now inadvertently brought into scope corporate systems and applications that do not meet the defined terms of an Applicable System. Since PACS are not required to be in an ESP, and remote access to them is not required to traverse through an Intermediate System, then there is no existing outer boundary used for remote access to PACS assets that is in-scope. FERC has not ordered adding PACS requirements to exactly the same requirements that apply to BCS as part of this Supply Chain initiative by merely changing the Applicable Systems column. There could be less restrictive requirements or new requirements based on

risk that could apply to PACS. We agree with the FERC Order and the NERC Study that there should be additional requirements for those PACS assets that perform “access control” functions and not merely monitoring and logging functions. Given the absence of an attempt to modify the NERC defined term for PACS to clarify the difference between PACS and PAMS, we do not agree with the addition of PACS at this time as the current definition of PACS assets to which these new requirements would apply is above and beyond the scope addressed in the FERC Order and the NERC Final Report. For these reasons, keeping requirements applicable to PACS in CIP-010 and CIP-013 addresses the FERC Order and NERC Study, however Southern believes the SDT should remove PACS from CIP-005 R2.4 and R2.5 until such time that the PACS definition can be modified and new definitions of applicable systems be added to properly scope these requirements.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity. At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “PACS, excluding those that provide only alerting and logging”, however, this change could introduce the requirement of maintaining “lists” of PACS and what functions they provide.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	

Dislikes 0	

Response

Thank you for your comment.

At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “PACS, excluding those that provide only alerting and logging”, however, this change could introduce the requirement of maintaining “lists” of PACS and what functions they provide.

The SDT agrees with the commenters’ statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the “Background” section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we agree with the addition of PACS to CIP-005, CIP-010 and CIP-013, we suggest that the SDT consider creating a new requirement, CIP-005-7 R3, and move Part 2.4 and Part 2.5 to this new requirement. We believe that this will help to alleviate any confusion that may exist surrounding PACS and Intermediate Systems.

Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	

CHPD believes that the PACS should not be added per the following discussion.

The Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019) recommended that PCAs be excluded from CIP-013-2 because 1) the risk is difficult to quantify and 2) there is not a direct 15-minute impact related to the PCA itself. The PCAs were excluded from CIP-010 and CIP-013, but included a recommendation to address them as a best practice.

PCAs, like PACS, have no direct 15-minute BES impact. PACS, unlike PCAs, do not reside within an ESP and have no network access to the BCS or related ESP. Therefore; if PCAs are not included, it seems logical for PACS to be treated in the same manner.

The NERC Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019) reasoned that PCA could be excluded from CIP-010 and CIP-013 due to the following:

1. *"The potential risk can be mitigated in part by technical controls, some of which are addressed in the CIP Reliability Standards and others which can be addressed in policies and procedures. For example, implementing access control lists, intrusion prevention systems, and malicious software prevention tools can be used to limit the risk posed by PCAs possibly impacting interconnected BES Cyber Systems" (p. 21).*
2. *The recommendation was to not include PCAs as "other controls deployed on the BES Cyber Systems under the CIP-007 and CIP-010 standards would protect the actual assets that could have a 15-minute impact if rendered unavailable, degraded, or misused" (p. 22).*

In conclusion, CHPD agrees with the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019) recommendation to exclude PCAs in favor of a best practice approach and adequate cyber security controls. CHPD recommends that this same reasoning be extended to PACS due to the lower potential risk to the BES.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT discussed this inclusion extensively and ultimately decided to include PACS. A review of the NERC Supply Chain Report also provides rationale for the inclusion of PACs. Specifically, the report details the following on page 24: “A compromise of PACs could allow access to systems that directly affect the operation of the BES, potentially allowing a threat source to negatively impact the BES reliability. Examples of scenarios application to compromised PACS components (such as those described above) include, but are not limited to, the following: A combined cyber/physical attack on one or more high impact BES Cyber Systems and their host Facilities, where external control of previously compromised PACS elements cold allow external threat actors to obtain undetected physical access to Control Centers and other Faculties that control or operate significant portions of the grid. Once inside the PSP, threat actors could detain, subvert, or eliminate the system operators and take physical control of the BES Cyber Systems.”	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GSOC and GTC do not agree with or support the addition of PACS to the applicable systems for the supply chain reliability standards. In particular, GSOC and GTC are concerned regarding NERC’s conclusion in Chapter 3 of the Supply Chain Risks report that “*…if compromised, misused, or rendered unavailable, PACS components could have a real-time impact on the reliability of the BES*” because the conclusion is inconsistent with the current classification of PACS components in a category distinct from BES Cyber Assets, and because a compromise of a PACS would not have a real-time impact on the BES without a secondary action.	

In accordance with the typical implementation of reliability standard CIP-002-5.1a and pursuant to the NERC-approved definition, if a cyber asset has or could have a direct impact on the reliability of the BES, it ***must be characterized*** as a BES Cyber Asset. A BES Cyber Asset is defined “[a] *Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed,* ***would affect the reliable operation of the Bulk Electric System****. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.”* Importantly, cyber assets that are classified as PACS are classified as such because they perform unique functions required by the CIP reliability standards, including, but not limited to CIP-006, CIP-004, etc. Hence, where responsible entities identify 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,” such cyber assets are appropriately classified as PACS. Thus, it is difficult to reach the same conclusion as NERC and the SDT, e.g., that a compromise, misuse, or rendering unavailability to PACS components would directly affect the reliable operation of the BES.

More importantly, though, these definitions form the foundation of cyber asset classification and the overall industry interpretation of how its cyber assets should be classified. The assertion by NERC that PACS directly impact the reliability of the BES and the SDT’s acceptance of this to justify their inclusion in the applicability for the supply chain reliability standards effectively upends nearly a decade of Commission, ERO, and industry precedent regarding what constitutes a BES Cyber Asset and what constitutes supporting cyber assets such as PACS.

GSOC and GTC acknowledge that the compromise, misuse, or rendering unavailable of PACS could be an initiating action for a secondary action of compromise, misuse, or rendering unavailable of a BES Cyber Asset or other cyber asset when determining adverse impact to the reliability of the BES. However, the singular, isolated cyber compromise to PACS without other secondary action does not and would not have real-time impacts on the reliability of the BES. More specifically, without a concurrent or subsequent physical compromise, the compromise, misuse, or rendering unavailable of a PACS alone cannot have a direct impact on the reliability of the BES. A second order of physical presence by way of entry into the Physical Security Perimeter must occur to impact reliability.

The inclusion of secondary actions when determining direct impacts is atypical generally and is also inapposite to the risk-based nature of the CIP reliability standards, the BES Cyber Asset definition, and the significance of asset redundancy as a risk mitigating strategy. The need for a secondary action (physical security compromise) and – potentially- a tertiary action (e.g., the compromise, misuse, or rendering unavailable of a BES Cyber Asset or BES asset equipment) clearly demonstrates that adverse action to PACS alone cannot directly impact the reliability of the BES. Given this reality, PACS would not and should not (in the CIP reliability standards risk based framework) require the same protections as those cyber assets that could directly impact the reliability of the BES.

NERC correctly refers to various Reliability Standards that mitigate security risks relating to PACS. These include CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GSOC and GTC assert that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GSOC and GTC oppose the inclusion/addition of PACS to the supply chain reliability standards. While GSOC and GTC 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

The SDT appreciates the thorough nature of this comment and evaluated the points raised. 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.

The commenter seems 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.

In regard to the attempt to draw a parallel between the 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.

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

Answer	No
Document Name	

Comment

It’s not clear what risk this is mitigating. Critical sites have additional protections (security guards) that are in place and will continue to provide visibility where needed in the event someone obtains unauthorized remote access to PACS.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment. The SDT discussed this inclusion extensively and ultimately decided to include PACS. A review of the NERC Supply Chain Report also provides rationale for the inclusion of PACs. Specifically, the report details the following on page 24:

“A compromise of PACs could allow access to systems that directly affect the operation of the BES, potentially allowing a threat source to negatively impact the BES reliability. Examples of scenarios application to compromised PACS components (such as those described above) include, but are not limited to, the following:

A combined cyber/physical attack on one or more high impact BES Cyber Systems and their host Facilities, where external control of previously compromised PACS elements cold allow external threat actors to obtain undetected physical access to Control Centers and other Faculties that control or operate significant portions of the grid. Once inside the PSP, threat actors could detain, subvert, or eliminate the system operators and take physical control of the BES Cyber Systems.”

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment	
Although the CAISO acknowledges that PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on wait with extending the program to PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from audit experiences including findings and areas of concerns identified by the auditors. At that time the CAISO also proposes 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	
The SDT thanks you for your comment, however, FERC order 850 has an implicit deadline of December 1, 2020.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
We agree conceptually on the intent but wonder if there is a real benefits on the overall electric reliability.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No

Document Name	
Comment	

1. The **NERC Cyber Security Supply Chain Risks** white paper recommendations excludes a) EACMS which provide monitoring and logging and b) PACS which perform alarming and logging services. The applicability and definitions in the revisions do not distinguish between preventive (firewalls) and detective (monitoring/alarming/logging) EACMS and PACS. This leads to confusion when identifying and developing procedures for cyber assets in or out of scope, when determining compliance to the standard, and at audits or when processing risk, cause, corrective and enforcement actions.

Recommend either removing the references in all revisions or revise the SAR to include a separate class of Cyber Systems which perform either the preventive control (IPS, Firewalls) or detective control functions (IDS, logging and alerting)

2. The “Applicable Systems” language does not distinguish between medium EACMS and PACS with ERC, however ERC is a consideration when classifying systems in the Parts.

Recommend initiating a revision to the Applicable Systems and Parts to address only a) EACMS and PACS with ERC as follows:

"Physical Access Control Systems (PACS) with External Routable Connectivity – Applies to each Physical Access Control System with ERC and associated with a referenced high impact or medium impact BES Cyber System"

"Electronic Access Control or Monitoring Systems (EACMS) with External Routable Connectivity – Applies to each Electronic Access Control or Monitoring System with ERC and associated with a referenced high or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems."

3. CIP-010-4 – “Applicable Systems” – PACS (pp5-6) includes for PACS “except as provided in Requirement R1, Part 1.6.” This is confusing and potentially adds Cyber Systems into scope which are not in scope

Recommend updating the Applicable Systems definitions to match the Parts where ERC is or is not required.

4. CIP-010-4 Part R1.6 – does not distinguish BCS with ERC from BCS without – in context, adds Cyber Systems to this requirement which are not in scope for the FERC Order 850 or NERC Cyber Security Supply Chain Risks white paper

Likes 0	

Dislikes 0	
Response	
The SDT thanks you for your comment. At this time there is no separation of access control vs. monitoring within the approved definition of EACMS or PACS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS or PACS is outside the SAR for this SDT due to EACMS and PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “PACS, excluding those that provide only alerting and logging” or “EACMS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and PACS and what functions they provide. The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 of CIP-010-4 and determined it was unnecessary. Please see the redline draft of CIP-010-4.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE agrees conceptually with including PACS but needs to assess the risk and implementation. However, we expect a lower return on investment on PACS. There should be some awareness message on the change for CIP-010-4 R1.6 on third party or shared infrastructure. Was it intentional to not capitalize electronic access point in CIP-005 R2.5 bullet three of the measures? We agree with the proposed changes. *We do see one issue with the change to the applicability of PACS on page 6 of the redlined standard document for CIP-010-4. We question whether the exception should be added or maybe it needs to also include part 1.1. I’m not sure it makes sense to include additional devices in part 1.6 that are not included in 1.1 given that 1.6 must be followed only when there is a change to the baseline defined in 1.1*	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting. Those with shared infrastructure (co-located or jointly owned BES facilities) need to review and reevaluate their agreements based on new or revised requirements. The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2. The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	

Comment

Alliant Energy does not oppose the addition of PACS, but agrees with the NSRF that consideration and clarity is needed around Medium Impact BES Cyber Systems with and without External Routable Connectivity.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT agrees with the commenters’ statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the “Background” section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

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

Answer	No
Document Name	

Comment

PG&E agrees with the addition of PACS but does not agree with the use of PACS as currently defined in the “Applicable System Columns in Tables” section of the Standard. Including PACS which only provide monitoring or alerting capabilities in the modifications extends what was indicated in the NERC supply chain study recommendation which indicated only “access control” capabilities. PG&E believes the risk of PACS which “only” provides monitoring and alerting capabilities is not the same as those which provide “access control” capabilities and should be excluded from the Standard. PG&E does indicate if a PACS provides access control while at the same time monitoring and/or alerting capabilities it should be covered by the Standard.

PG&E recommends the definition in the “Applicable System Columns in Tables” section be altered to indicate only those PACS which provide “access control” and that PACS that only provide monitoring and alerting be excluded. A Technical Rationale document could be created to clearly indicate what type of PACS would be covered with examples to help clarify any confusion. A potential benefit in making

the “Applicable Systems Column in Table” indicate PACS with only “access control” is to the Project 2016-02 SDT working on the separation of PACS into Cyber Assets for “access control” (PACS) and monitoring/alerting (PAMS). A clear indication of “access control” in the Project 2019-03 modifications could make it easier for the Project 2016.-02 SDT to make conforming changes to CIP-005, CIP-010, and CIP-013 once they are ready to complete the work on the PACS separation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “PACS, excluding those that provide only alerting and logging”, however, this change could introduce the requirement of maintaining “lists” of PACS and what functions they provide.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
We agree conceptually with including PACS but need to assess the risk and implementation. However, we expect a lower return on investment on PACS. There should be some awareness message on the change for CIP-010-4 R1.6 on third party or shared infrastructure. Was it intentional to not capitalize electronic access point in CIP-005 R2.5 bullet three of the measures?	
Likes 0	
Dislikes 0	

Response

Thank you for your comment.

The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting. Those with shared infrastructure (co-located or jointly owned BES facilities) need to review and reevaluate their agreements based on new or revised requirements.

The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports RSC comments.

Likes 0	
Dislikes 0	

Response

Thank you for your comment.

The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting. Those with shared infrastructure (co-located or jointly owned BES facilities) need to review and reevaluate their agreements based on new or revised requirements.

The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC and GTC do not agree with or support the addition of PACS to the applicable systems for the supply chain reliability standards. In particular, GSOC and GTC are concerned regarding NERC's conclusion in Chapter 3 of the Supply Chain Risks report that "*…if compromised, misused, or rendered unavailable, PACS components could have a real-time impact on the reliability of the BES*" because the conclusion is inconsistent with the current classification of PACS components in a category distinct from BES Cyber Assets, and because a compromise of a PACS would not have a real-time impact on the BES without a secondary action.

In accordance with the typical implementation of reliability standard CIP-002-5.1a and pursuant to the NERC-approved definition, if a cyber asset has or could have a direct impact on the reliability of the BES, it ***must be characterized*** as a BES Cyber Asset. A BES Cyber Asset is defined "[a] *Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed,* ***would affect the reliable operation of the Bulk Electric System***. *Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.*" Importantly, cyber assets that are classified as PACS are classified as such because they perform unique functions required by the CIP reliability standards, including, but not limited to CIP-006, CIP-004, etc. Hence, where responsible entities identify 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," such cyber assets are appropriately classified as PACS.   Thus, it is difficult to reach the same conclusion as NERC and the SDT, e.g., that a compromise, misuse, or rendering unavailability to PACS components would directly affect the reliable operation of the BES.

More importantly, though, these definitions form the foundation of cyber asset classification and the overall industry interpretation of how its cyber assets should be classified. The assertion by NERC that PACS directly impact the reliability of the BES and the SDT's acceptance of this to justify their inclusion in the applicability for the supply chain reliability standards effectively upends nearly a decade of Commission, ERO, and industry precedent regarding what constitutes a BES Cyber Asset and what constitutes supporting cyber assets such as PACS.

GSOC and GTC acknowledge that the compromise, misuse, or rendering unavailable of PACS could be an initiating action for a secondary action of compromise, misuse, or rendering unavailable of a BES Cyber Asset or other cyber asset when determining adverse impact to the reliability of the BES. However, the singular, isolated cyber compromise to PACS without other secondary action does not and would not have real-time impacts on the reliability of the BES. More specifically, without a concurrent or subsequent physical compromise, the compromise, misuse, or rendering unavailable of a PACS alone cannot have a direct impact on the reliability of the BES. A second order of physical presence by way of entry into the Physical Security Perimeter must occur to impact reliability.

The inclusion of secondary actions when determining direct impacts is atypical generally and is also inapposite to the risk-based nature of the CIP reliability standards, the BES Cyber Asset definition, and the significance of asset redundancy as a risk mitigating strategy. The need for a secondary action (physical security compromise) and – potentially- a tertiary action (e.g., the compromise, misuse, or rendering unavailable of a BES Cyber Asset or BES asset equipment) clearly demonstrates that adverse action to PACS alone cannot directly impact the reliability of the BES. Given this reality, PACS would not and should not (in the CIP reliability standards risk based framework) require the same protections as those cyber assets that could directly impact the reliability of the BES.

NERC correctly refers to various Reliability Standards that mitigate security risks relating to PACS. These include CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GSOC and GTC assert that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GSOC and GTC oppose the inclusion/addition of PACS to the supply chain reliability standards. While GSOC and GTC 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 comment. Please see response at the beginning of Q2, which is also included in Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO

Answer	No
Document Name	

Comment

We agree with the addition of PACS (and EACMS) to CIP-005-7 and CIP-013-2, but a close examination of the currently approved definition(s) of PACS (and EACMS) prevents them from being added to Medium Impact BES Cyber Systems in CIP-010-4 Requirement R1, Part 1.6 as proposed.

PACS are currently defined as:

“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.”

PACS are tied to PSPs. PSPs only exist with respect to Medium Impact BES Cyber Systems for those with ERC per CIP-006-6 Requirement R1, Part 1.2. Medium Impact BES Cyber Systems without External Routable Connectivity are only required to define operational or procedural controls to restrict physical access; a PACS is not required.

We recommend, for clarity and consistency among CIP standards:

1.) Insert:

“Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS; and

2. PACS”

Between High Impact and Medium Impact Applicable Systems in CIP-010-4 Requirement R1, Part 1.6.

2.) Delete “except as provided in Requirement R1, Part 1.6” from the PACS description in the Background on p. 6.

Although the PACS applicability language does not directly affect CIP-005-7, we recommend that the new inclusion of PACS applicability in the Background on p. 6 include "with External Routable Connectivity" to be consistent with most of the standards. CIP-006-6 and CIP-007-6 should likewise be corrected during the next revision.

CIP-006-6 and CIP-007-6 language:

"Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System."

CIP-004-6, CIP-009-6, CIP-010-3 and CIP-011-2 language:

"Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity."

Also, in keeping with the same principle, for CIP-013-2, we suggest changing Requirement R1, "for high and medium impact BES Cyber Systems and their associated EACMS and PACS," to "for high and medium impact BES Cyber Systems, and EACMS and PACS associated with high impact BES Cyber Systems or medium impact BES Cyber Systems with External Routable Connectivity."

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Thank you for your comment.

At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "PACS, excluding those that provide only alerting and logging", however, this change could introduce the requirement of maintaining "lists" of PACS and what functions they provide.

The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered

Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the “Background” section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

We agree to add PACS to the applicable systems but disagree with the language regarding PACS in CIP-013-2 R1 and CIP-010-4 Section 6 Background since it would bring PACS associated with BCS w/o ERC into scope. Currently It has been commonly understood that only PACS associated with BCS with ERC is applicable to the CIP standards based on CIP-006 R1.1 requirement in which PACS is not required for medium impact BCS without ERC. We suggest making the following changes:

For CIP-013-2 R1, Part 1.1 and Part 1.2, change “high and medium impact BES Cyber Systems and their associated EACMS and PACS” to “high and medium impact BES Cyber Systems and their associated EACMS, and PACS associated with high impact BES Cyber Systems or medium impact BES Cyber Systems with External Routable Connectivity.”

For CIP-010-4, remove the wording “except as provided in Requirement R1, Part 1.6.” from Section 6 Background.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT agrees with the commenters’ statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the “Background” section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Adding PACs is not necessary. The standards as they are right now are just fine.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Adding PACS is not necessary. The standards as they are right now are just fine.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
sean erickson - Western Area Power Administration - 1	

Answer	No
Document Name	

Comment

The **NERC Cyber Security Supply Chain Risks** white paper recommendations excludes a) EACMS which provide monitoring and logging and b) PACS which perform alarming and logging services. The applicability and definitions in the revisions do not distinguish between preventive (firewalls) and detective (monitoring/alarming/logging) EACMS and PACS. In addition, the Applicable Systems and language does not distinguish between EACMS and PACS with ERC. Recommend revising Definitions, Applicable Systems and Parts to address only EAMCS and PACS with ERC and which perform preventive security services.

CIP-010-4 – Applicable Systems – PACS (pp5-6): current term of a PACS “except as provided in Requirement R1, Part 1.6.” adds Cyber Systems into scope which are not in scope. It is not clear and confusing.

CIP-010-4 R1.6 – does not distinguish BCS with ERC from BCS without – in context, adds Cyber Systems to this requirement which are not in scope for the FERC Order 850 or NERC Cyber Security Supply Chain Risks white paper

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Thank you for your comment. At this time there is no separation of access control vs. monitoring within the approved definition of EACMS or PACS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS or PACS is outside the SAR for this SDT due to EACMS and PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “PACS, excluding those that provide only alerting and logging” or “EACMS, excluding those that provide only monitoring and logging”:, however, this change could introduce the requirement of maintaining “lists” of EAMCS and PACS and what functions they provide.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.

The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NO. Adding PACS is not necessary. The Standards as they are right now are just fine.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Tampa Elecric does not oppose the addition of PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI does not oppose the addition of PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
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, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	

Answer	Yes
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
The IRC SRC requests clarification. Was it the SDT's intent not to capitalize "electronic access point" and "intermediate system" under CIP-005-7, requirement R2, part 2.5, bullet three under Measures? NYISO doesn't understand the applicability for controls for remote access regarding PACS devices as implied within CIP-005 remote access requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2. The SDT has moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity around remote access requirements.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and does not oppose the addition of PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Duke Energy generally agrees with adding PACS to the Supply Chain Standards as currently described above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
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	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
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	
Glen Farmer - Avista - Avista Corporation - 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	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
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	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 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	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
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	

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Cynthia Lee - Exelon - 5	
Answer	

Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

3. Based on the addition of PACS to CIP-005 R2.4 and R2.5 and the lower risk they pose to the BES, the SDT has modified the associated VSL's. A violation of failing to have a method for determining OR disabling for PACS is listed as a Moderate VSL, and a violation of failing to have a method for determining AND disabling is listed as a High VSL. Do you agree with the modified VSLs? If you do not agree, please explain and provide your recommendation.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NO. They should be low, or better yet not a violation at all.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. Since PACS are listed in the requirement language, there must be an associated reference to them in the VSL so they cannot be removed completely. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
They should be low, or better yet not a violation at all.	

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. Since PACS are listed in the requirement language, there must be an associated reference to them in the VSL so they cannot be removed completely. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
They should be low, or better yet not a violation at all.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Since PACS are listed in the requirement language, there must be an associated reference to them in the VSL so they cannot be removed completely. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Since PACS poses a lower risk to the BES, Duke Energy suggests that the VSLs should be lowered and should be no higher than Low or Moderate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Since PACS are listed in the requirement language, there must be an associated reference to them in the VSL so they cannot be removed completely. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	
We agree with the modified VSLs, but believe there are underlying problems with CIP-005-7 R2.4 and R2.5 as currently proposed. 1.) The requirements assume vendor remote access sessions and impose additional monitoring requirements upon all Responsible Entities regardless of whether or not a Responsible Entity permits vendor remote access sessions. There is no need for this ongoing requirement if an entity decides not to permit vendor remote access sessions and has ensured that such sessions are either blocked or not able to be established. We recommend R2.4 be changed to add the following, or equivalent language, before the parenthesis: "… where permitted and not otherwise blocked or unable to be established…" R2.5 can then be changed to add "according to R2.4 above" before the parenthesis.	

2.) Per the Background Information provided at the beginning of this comment form, we propose the following change to the Applicable Systems for R2.4 and R2.5 as a means of meeting the NERC supply chain report recommendations to include (i) EACMS that provide electronic access control (excluding monitoring and logging) (p. 7), and (ii) PACS that provide physical access control, excluding alerting and logging (p. 12) while retaining current definitions: Expand EACMS to “EACMS that provide electronic access control (excluding monitoring and logging),” or equivalent language. Expand PACS to “PACS that provide physical access control (excluding alerting and logging)”	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. The SDT has provided draft guidance around scenarios where a Responsible Entity does not permit vender remote access sessions in CIP-005-7 Implementation Guidance. In response to EACMS and PACS definitions, please see response to MRO from questions 1 and 2 above.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
While GSOC and GTC agree that the VSLs and VRFs associated with the addition of PACS should be lower, as discussed above, GSOC and GTC disagree with the addition of PACS to these requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to GSOC and GTC from questions 1 and 2 above.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	

Comment

The wording is awkward and should be clarified to explain that failing to have one of the two methods required (determining OR disabling) is a moderate VSL while failure to have any of the required methods (lacking BOTH a means to determine and lacking a means to disable) is a high VSL.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT modified the VSL language to make this distinction clearer. Please note, the previous CIP-005-7 R2.4 and R2.5 have now been moved to R3.

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant Energy agrees with the modified VSLs, but agrees with the NSRF that the language should be clarified for the scenario where a Responsible Entity does not permit vendor remote access sessions for some or all vendors.

Alliant Energy also supports the NSRF’s comments to update the applicability section to include only EACMS that provide electronic access control (excluding monitoring and logging) and PACS that provide physical access control (excluding alerting and logging).

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT has provided draft guidance around scenarios where a Responsible Entity does not permit vender remote access sessions in CIP-005-7 Implementation Guidance. In reference to EACMS and PACS definitions, please see responses to MRO in questions 1 and 2 above.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE disagrees with adding EACMS and PACS to CIP-005. CIP-005 was intended for access to High and PCA systems. In fact, EACMs are derived from the CIP-005 requirements. The CIP standards and requirements are structured to address security concerns based on the criticality and risk to the BES. EACMS and PACS do not incur the same security concerns and do not have the same criticality or risk to the BES; therefore, EACMS and especially PACS should not be treated the same as High or Medium Impact systems that have a	

direct correlation to the reliability of the BES. Additionally, the co-mingled definition of “access control and monitoring” inherently elevates systems with monitoring only capability to a high-water mark, adding the need to incorporate burdensome and costly controls to extremely low risk systems for little benefit. In support of the lower impact and risk, both VSLs should be listed as minimal to moderate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2. In reference to EACMS and PACS, please see response from question 1.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
Due to the low risks Vendor remote access to PACS have to the operation of the BES, we feel the VSLs should be the lowest possible. The protections and requirements already afforded to Vendor remote access to PACS: access control, PRAs, training, etc., already reduce the risks PACS pose to the BES. The new requirements are a best practice, and do not have a high enough risk level to warrant a Medium or High VSL.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3

Answer	No
Document Name	

Comment

Agree with Duke Energy's comment.

"Since PACS poses a lower risk to the BES, Duke Energy suggests that the VSLs should be lowered and should be no higher than Low or Moderate."

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

Although the CAISO acknowledges that PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from

audit experiences including findings and areas of concerns identified by the auditors. At that time the CAISO also proposes 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	
The SDT thanks you for your comment, however, FERC order 850 has an implicit deadline of December 1, 2020.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
If PACS was added, which I disagree with, the modified VSLs can help at the time of enforcement, but don't help during implementation. VSLs are not evaluated when determining how to implement CIP requirements and VSLs do not influence the level of effort applied to protect the BES.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	

We agree with the modified VSLs, but believe there are underlying problems with CIP-005-7 R2.4 and R2.5 as currently proposed.

1.) The requirements assume vendor remote access sessions and impose additional monitoring requirements upon all Responsible Entities regardless of whether or not a Responsible Entity permits vendor remote access sessions. There is no need for this ongoing requirement if an entity decides not to permit vendor remote access sessions and has ensured that such sessions are either blocked or not able to be established.

We recommend R2.4 be changed to add the following, or equivalent language, before the parenthesis:

"… where permitted and not otherwise blocked or unable to be established…"

R2.5 can then be changed to add "according to R2.4 above" before the parenthesis.

2.) Per the Background Information provided at the beginning of this comment form, we propose the following change to the Applicable Systems for R2.4 and R2.5 as a means of meeting the NERC supply chain report recommendations to include (i) EACMS that provide electronic access control (excluding monitoring and logging) (p. 7), and (ii) PACS that provide physical access control, excluding alerting and logging (p. 12) while retaining current definitions:

Expand EACMS to "EACMS that provide electronic access control (excluding monitoring and logging)," or equivalent language.

Expand PACS to "PACS that provide physical access control (excluding alerting and logging)"

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT has provided draft guidance around scenarios where a Responsible Entity does not permit vender remote access sessions in CIP-005-7 Implementation Guidance. Please see responses to PACS and EACMS definitions in questions 1 and 2.

Greg Davis - Georgia Transmission Corporation - 1

Answer	No

Document Name	
Comment	
While GSOC and GTC agree that the VSLs and VRFs associated with the addition of PACS should be lower, as discussed above, GSOC and GTC disagree with the addition of PACS to these requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to GSCO and GTC in questions 1 and 2 above.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to MRO in questions 1 and 2 above.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	

Based on response under question #2 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to question 2 above.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see responses to MRO in questions 1 and 2 above.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
No Comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the indicated VSL assignments for PACS.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Xcel Energy supports EEI comments and does not oppose the changes to VSLs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
NYISO doesn’t understand the applicability for controls for remote access regarding PACS devices as implied within CIP-005 remote access requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity around vendor remote access.	
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, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	

Answer	Yes
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
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)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to questions 1 and 2 above.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the modifications made to the VSLs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the modifications to the VSL's. However, see our comments in questions 1 and 2 with regard to the addition of EACMS and PACS assets to the scope of these new requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see response to questions 1 and 2 above.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes

Document Name	
Comment	
Tampa Elecric supports the modifications made to the VSLs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
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	
Tim Womack - Puget Sound Energy, Inc. - 3	
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	
sean erickson - Western Area Power Administration - 1	
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	
Anthony Jablonski - ReliabilityFirst - 10	
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	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
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	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
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	

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	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
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 RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
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	
Jeff Icke - Colorado Springs Utilities - 5	
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	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

4. The SDT is proposing a 12 month implementation plan. Do you agree with the proposed timeframe? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

SDT General Response to Question 4

Thank you for your comment, there have been significant discussions referring to the comments proposed by EEI and their recommendation. It has been proposed that the SDT expand 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 covered under existing contracts.
- 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, outside of the EEI recommendations, other entities have 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 would include but not limited to:

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

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.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No

Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
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 4.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	

We would prefer an 18 month implementation to better accommodate a budget cycle	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Tampa Elecric supports EEI recommendation that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, the additional time to implement the standard is necessary.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	

Comment	
Eversource suggests an 18-month implementation plan due to current experience with adding vendors to the initial Supply Chain project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	
We recommend a longer implementation period than the proposed 12 months.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
NPCC recommends an 18 or 24 month Implementation Plan due to entity budget cycles and significant increases in scope for the entity.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of 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 recommends that the SDT expand the proposed time for implementation plan to 18 months and suggests for the SDT to consider budget cycles for possible technological upgrades needed before implementation. In this case, 18 months would be a fair alternate time frame. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, the additional time to implement the standard is necessary.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No

Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI recommends that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, the additional time to implement the standard is necessary.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of 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, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	No
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 4	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	No
Document Name	
Comment	
The IRC SRC recommends an 18- or 24-month Implementation Plan to allow sufficient lead time for an entity to incorporate changes into their programs as time will be needed to justify costs and obtain budgets as well as developing approaches to accommodate the expansion of assets included in scope. Depending upon how an entity implemented 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 will need to develop and implement a different process for EACMS and PACS systems. Therefore, the IRC SRC requests the SDT allow additional time. Note: CAISO (segment 2, WECC region) also joins the IRC SRC in the comments provided in response to Question 4.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports EEI comments on this question and believes that an 18 month implementation period would be more appropriate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GSOC and GTC do not agree that the addition of EACMS to the Supply Chain Standards is only administrative in nature. The current applicability consists only of High and Medium Impact BES Cyber Systems and associated Protected Cyber Assets. The nature and makeup of systems that perform the function of electronic access control are materially different than those that perform functions of BES Cyber Systems. For instance, consider a substation environment. One can reasonably envision a program that consists entirely of protective relays, remote terminal units, data concentrator, carrier radios, etc. Note that the nature of all of these systems are	

embedded. Introduction of electronic access control systems introduces entirely new classes of infrastructure, including software that may not even be considered in an entity’s existing program. Therefore, we strongly disagree with the assertion that the changes are administrative.

Furthermore, budgeting and planning efforts within most electric utility organizations occur at least annually with budget and/or project planning and finalization for each year occurring in advance of the implementing year. Often, major system replacements and upgrades are planned more than a year in advance of the anticipated implementing year. Further, responsible entities with contract/procurement management systems that are facilitating their CIP-013 compliance may have technical/programming needs to modify these corporate procurement systems to include EACMS for compliance reporting purposes.

For these reasons, GSOC and GTC recommend 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 4.

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

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

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	
Comment	
MPC does not agree that the addition of EACMS to the Supply Chain Standards is only administrative in nature. Budgeting and planning efforts within most electric utility organizations occur at least annually with budget and/or project planning and finalization for each year occurring in advance of the implementing year. Often, major system replacements and upgrades are planned more than a year in advance of the anticipated implementing year. Further, responsible entities with contract/procurement management systems that are facilitating their CIP-013 compliance may have technical/programming needs to modify these corporate procurement systems to include EACMS for compliance reporting purposes. For these reasons, MPC recommends an 18 month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
Because EACMS and PACS may be located outside of any Electronic Security Perimeter (Intermediate Systems MUST be outside any ESP), N&ST believes entities *could* find it necessary to define and implement controls for CIP-005 R2.4 and R2.5 for EACMS and PACS that are entirely different than the ones they have implemented for BES Cyber Systems and PCAs. Therefore, N&ST believes the implementation plan duration should be 18 months, not 12 months.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24 month implementation plan after the applicable governmental entity’s order approving the standard to allow entities flexibility to determine the appropriate implementation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The proposed implementation timeline may not allow enough time for industry to properly gauge the effects of the preceding version of standards Subject to Enforcement. Based on the outcomes of the yet to become effective versions of the Standards, additional budget and time could be needed to implement the proposed updates. SRP would like to recommend an implementation timeline of 15 to 18 calendar months, starting in the next calendar quarter of the approval of CIP-005-7, CIP-010-4, and CIP-013-2.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
The IRC SRC recommends an 18 or 24-month Implementation Plan to allow sufficient lead time for an entity to incorporate changes into their programs as time will be needed to justify costs and obtain budgets as well as developing approaches to accommodate the expansion of assets included in scope. Depending upon how an entity implemented 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 will need to develop and implement a different process for EACMS and PACS systems, so the IRC SRC requests the SDT allow additional time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
Considering the scope of changes introduced by SDT, we recommend an 18 or 24 month implementation plan.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Jamie Prater - Entergy - 5	
Answer	No
Document Name	
Comment	
Entergy proposes an 18 month implementation plan as was approved via Project 2016-03 for these standards. While the requirement language does not change, the inclusion of systems that were not originally included in the Project 2016-03 scope should allow for the same timeline of implementation as entities must again evaluate compliance strategies for new sets of hardware and/or software that may not be compatible with the entity's expected processes for BCA and PCA assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Agree with Duke Energy's comment. "Duke Energy recommends a 24-month implementation plan as technical upgrades are likely necessary to meet the Reliability Standards' security objectives, which could involve a longer time-horizon, capital budgets and planning cycles."	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
18 months minimum	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Although adding the words EACMs and PACS to the requirements seems fairly innocuous. It can in fact be a significant impact to an Entity's CIP compliance program and approach. Entities may need to evaluate, procure and implement new technologies and processes to incorporate these systems.	

Recommend a 24 month implementation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments recommending that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors,	

entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
From participation NERC and industry discussions, it appears that the basis for a 12-month implementation centers on an assumption that EACMS and PACS vendors are the same for high 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 (control center) and medium (ex. substation) impact environments are very different. CEHE suggest that 12 months is not sufficient and would like to propose 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 4.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	

Comment	
FE recommends that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS will result in a significant expansion in scope for both hardware and software covered under existing contracts. Entities will need to modify existing policies and processes and negotiate modified contracts with existing vendors to cover new equipment and systems. In addition, these new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, we feel additional time will be required to implement the standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
NPCC recommends an 18 or 24 month Implementation Plan due to entity budget cycles and significant increases in scope for the entity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No

Document Name	
Comment	
The addition of system-to-system access will take defining and further investigation; BPA believes this is a larger change than we can accomplish in 12 months. Also, Projects 2016-02 and 2019-03 definitions and implementation dates must be reconciled.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports RSC comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

GSOC and GTC do not agree that the addition of EACMS to the Supply Chain Standards is only administrative in nature. The current applicability consists only of High and Medium Impact BES Cyber Systems and associated Protected Cyber Assets. The nature and makeup of systems that perform the function of electronic access control are materially different than those that perform functions of BES Cyber Systems. For instance, consider a substation environment. One can reasonably envision a program that consists entirely of protective relays, remote terminal units, data concentrator, carrier radios, etc. Note that the nature of all of these systems are embedded. Introduction of electronic access control systems introduces entirely new classes of infrastructure, including software that may not even be considered in an entity's existing program. Therefore, we strongly disagree with the assertion that the changes are administrative. Furthermore, budgeting and planning efforts within most electric utility organizations occur at least annually with budget and/or project planning and finalization for each year occurring in advance of the implementing year. Often, major system replacements and upgrades are planned more than a year in advance of the anticipated implementing year. Further, responsible entities with contract/procurement management systems that are facilitating their CIP-013 compliance may have technical/programming needs to modify these corporate procurement systems to include EACMS for compliance reporting purposes. For these reasons, GSOC and GTC recommend a 24 month implementation plan.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	
The NSRF recommends an overall 18-month implementation plan. The SDT is already changing yet to be effective Standards whereby applicable entities will need to prove compliance then add additional compliance attributes (PACS and EACMS). There may be new	

entities who will need to start a new portion of their compliance program to satisfy these new attributes. Recommend an 18-month implementation plan.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends a 24-month implementation plan as technical upgrades are likely necessary to meet the Reliability Standards' security objectives, which could involve a longer time-horizon, capital budgets and planning cycles.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Should be 48 months or longer.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Should be 48-months or longer.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
We propose an 18 month implementation plan in order to address change management: understand the impact to existing programs, processes and documentation, revise existing documentation, develop and implement changes and test changes for integrity.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NO. Should be 48-months, or longer.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
ATC reccommends the SDT modify the current implementation plan to allow entities 18 months to fully implement the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	

Answer	No
Document Name	
Comment	
18 month is more reasonable since 12 month will be hard for entities that have many vendors to meet the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
Some smaller entities may not have the resouces or time to allocate with only a one year implementation. Typically our budgets are very tight and are set one year in advance, in October. A longer implementaiton time assures we have resouces that can be allocated through the annual budget process.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	

Comment	
Support the MRO comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI's recommendation that the SDT expand the proposed time for the implementation plan to 18 months.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the proposed 12-month implementation plan. PG&E believes the Cyber Assets being brought into scope for this modification should be able to follow the same plans and processes being developed for the BES Cyber Systems (BCS) under CIP-013-1. PG&E does not anticipate significant changes to the plans or processes would need to be done exempt for an indicating that EACMS and PACS must be covered, and believes the education of personnel handling the procurement and implementation of the Part 1.2 controls for EACMS and PACS should be able to be done within the 12-month interval.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
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	
Jeff Icke - Colorado Springs Utilities - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 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	
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	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
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	
Tim Womack - Puget Sound Energy, Inc. - 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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Cynthia Lee - Exelon - 5	

Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	

5. 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.

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The costs associated with ensuring supply chain and CIP-010 R1.6 and CIP-013 R1.2.5 - integrity of software in the supply chain, as well as the requirement to have multi-departmental personnel, updates to existing documentation, new documentation, changes to systems and contract changes will cost industry and ratepayers many thousands of dollars in personnel, systems and process work.

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

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.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

NERC needs to include the real costs of all new regulations they are imposing not the low ball figures they have provided in the past.

The costs impacts on entities due to the constant changing of Standards and having entities change documents we just changed needs to be included. Lost productivity time cost of getting modified documents and budgets approved and implemented (once again due to NERC program changes) by our governing boards cost of lost opportunities!

Also they need to include costs for specific new FTEs (SMEs, persons to insure project controls in place, persons to quality check new controls). Plus they need to include cost of changing/Updating existing plans and policies, cost to send out new RFPs to Vendors, cost for additional/updated Vendor reviews per another set a CIP standards changes.

NERC is proposing these new changes when the Supply Chain Standard has not even taken effect yet nor have prior approved CIP-005 and 10 July 1, 2020 effectives versions.

And now they are proposing changes to these standards, again. They are working on more proposed changes, see project 2016-02. In my view all these multiple changes and proposals are unnecessary and costly to entities; let only confusing to use, our governing boards, and have little, if any, real reliability value.

Likes 0	
Dislikes 0	
Response	
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.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	

A scope change of applicable CIP system always cause additional compliance cost. We don’t know whether the current change is cost-effective or not.

Likes 0	
Dislikes 0	

Response

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.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO

Answer	No
Document Name	

Comment

One member entity estimated the following costs and provides a recommendation:

Depending on the entity, the costs associated with the proposed changes may range between an annualized cost of $80K (80 to 100 hours per person) and $500K per entity. This does not include capital expenditures for technologies which manage vendor access, which may exceed $5M per entity.

This is based on the need to:

a. Develop, update and implement procedures and training for multiple departments and their personnel.

b. Perform updates to existing categorization processes to ensure the identification and controls exist to meet and exceed the requirements in the revisions.

c. Identify existing or implement new technologies to manage supplier or vendor remote access solutions. This includes efforts in integration and changes to systems, contracts, processes and internal compliance program metrics.

Recommend utilizing existing CIP program processes to meet the requirements. For example, CIP-013 R1.5 requires software integrity in the supply chain. CIP-010 R1.6 requires software integrity. CIP-007 R2 also requires integrity in software security patches. Aligning those standards into a single meaningful standard could improve cost effectiveness.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
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.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
While GSOC and GTC 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. 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.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No

Document Name	
Comment	
BPA supports WAPA’s comment as follows: “The costs associated with ensuring supply chain and CIP-010 R1.6 and CIP-013 R1.2.5 - integrity of software in the supply chain, as well as the requirement to have multi-departmental personnel, updates to existing documentation, new documentation, changes to systems and contract changes will cost industry and ratepayers many thousands of dollars in personnel, systems and process work.”	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
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.	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E cannot agree the modifications are cost effective at this time. This is based on the current effort to implement CIP-013-1 has not been completed and a full understanding of the current costs is not known. PG&E would have preferred to answer this question as “Unknown”, but the option was not available.	
Likes 0	
Dislikes 0	
Response	

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.	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with the NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
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.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

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.	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
NERC should perform an impact analysis as part of the SAR process. Every change impacts existing documentation and process stacks.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
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.	

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
Although the CAISO acknowledges that EACMS and PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on wait with 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 a two years to allow for the processes and controls to mature, 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 CAISO also proposes 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	
The SDT thanks you for your comment, however, FERC order 850 has an implicit deadline of December 1, 2020.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The FERC order states this is only an "increased paperwork burden" which I disagree with. Where does this include the actual ongoing monitoring of activity and maintaining an adequate level of training personnel across multiple parts of the power systems that know how to respond?	
Likes 0	

Dislikes 0	
Response	
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.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Prior to proposing additional modifications, Reclamation recommends each SDT take additional time to effectively define the scope of each Standard Authorization Request to minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. This will provide entities economic relief by allowing technical compliance with current standards.	
Likes 0	
Dislikes 0	
Response	
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.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

While GSOC and GTC 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. 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.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
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.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	

Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
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.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
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.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	

Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
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 R2.4 and R2.5. 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. One suggestion would be to allow the additional time suggested in Question 4 to consider those budget cycles for any possible technology upgrades.	
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	

Re-use of existing terms is easier and more cost effective than introducing new terms and/or requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 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	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
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	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
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	

Anton Vu - Los Angeles Department of Water and Power - 6	
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	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
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	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	

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 RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. NERC needs to include the real costs of all new regulations they are imposing not the low ball figures they have provided in the past.	

The costs impacts on entities due to the constant changing of Standards and having entities change documents we just changed needs to be included. Lost productivity time cost of getting modified documents and budgets approved and implemented (once again due to NERC program changes) by our governing boards cost of lost opportunities!

Also they need to include costs for specific new FTEs (SMEs, persons to insure project controls in place, persons to quality check new controls). Plus they need to include cost of changing/Updating existing plans and policies, cost to send out new RFPs to Vendors, cost for additional/updated Vendor reviews per another set a CIP standards changes.

NERC is proposing these new changes when the Supply Chain Standard has not even taken effect yet nor have prior approved CIP-005 and 10 July 1, 2020 effectives versions.

And now they are proposing changes to these standards, again. They are working on more proposed changes, see project 2016-02. In my view all these multiple changes and proposals are unnecessary and costly to entities; let only confusing to use, our governing boards, and have little, if any, real reliability value.

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

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.

Scott Tomashefsky - Northern California Power Agency - 4

Answer	
Document Name	

Comment

NERC needs to include the real costs of all new regulations they are imposing not the low ball figures they have provided in the past.

The costs impacts on entities due to the constant changing of Standards and having entities change documents we just changed needs to be included. Lost productivity time cost of getting modified documents and budgets approved and implemented (once again due to NERC program changes) by our governing boards cost of lost opportunities!

Also they need to include costs for specific new FTEs (SMEs, persons to insure project controls in place, persons to quality check new controls). Plus they need to include cost of changing/Updating existing plans and policies, cost to send out new RFPs to Vendors, cost for additional/updated Vendor reviews per another set a CIP standards changes.

NERC is proposing these new changes when the Supply Chain Standard has not even taken effect yet nor have prior approved CIP-005 and 10 July 1, 2020 effectives versions.

And now they are proposing changes to these standards, again. They are working on more proposed changes, see project 2016-02. In my view all these multiple changes and proposals are unnecessary and costly to entities; let only confusing to use, our governing boards, and have little, if any, real reliability value.

Likes 0	
Dislikes 0	

Response

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.

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

No Comments.

Likes 0	

Dislikes 0	
Response	
Thank you for your response.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
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.	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. 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.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
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.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	

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.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy takes no position on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
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, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 5.	
Likes 0	
Dislikes 0	

Response	
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.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
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.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your 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	
Thank you for your response.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
Tampa Electric takes no position as to the cost effectiveness of the proposed changes	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

6. Provide any additional comments for the standard drafting team to consider, if desired.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
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 response to EEI for question 6 below.	

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
The proposed changes to include EACMS and PAC to the CIP-010-4 requirements seem reasonable, but will add to workload.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	

Document Name	

Comment

Tampa Electric supports the following EEI comments: In this draft, the SDT has chosen to include all EACMS while the Commission provided the SDT with enough latitude to include only those EACMS that represent a known risk to the BES. (see Order 850, P51 where the Commission states “[We] leave it to the standard drafting team to assess the various types of EACMS and their associated levels of risks. We are confident that the standard drafting team will be able to develop modifications that include only those EACMS whose compromise by way of the cybersecurity supply chain can affect the reliable operation of high and medium impact BES Cyber Systems.”) With this in mind, we encourage the SDT to reevaluate its approach and develop more targeted modification that only address the known risks associated with EACMS that perform the function of controlling electronic access.

In addition to the concerns stated above, EEI also disagrees with the change made to proposed Reliability Standard CIP-005-7, Requirement 2, Subpart 2.5. While on the surface the change might appear to address the order, the change can be interpreted in such a way that would create an untenable dilemma. The language can be read to obligate entities to not just terminate vendor access through methods such as disabling rules within a firewall or disabling a user account for EACMS (e.g., Windows domain controller) but also to require entities to block all vendor access to the EACMS itself (i.e., install a firewall for the firewall). Unfortunately, this solution is unworkable because the new firewall would become a new EACMS obligating the entity to again install another firewall creating an endless loop of new obligations (i.e., you’ve entered the “hall of mirrors”). To resolve this issue, we recommend simply removing PACS and EACMS from the applicability section of Requirement R2, Subpart 2.5.

EEI also urges the SDT to develop Implementation Guidance for Industry review and comment on the proposed changes. The changes offered raise many questions on how best to develop and implement solutions that achieve effective compliance. Such guidance will help entities to better understand the proposed changes offered by the SDT.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT

considered adding qualifying language to the standard such as “EACMS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide. The SDT has moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE seeks clarification as to why PACS and EACMS were not added as applicable systems for Parts 2.1-2.3. In the scenario where a vendor is utilizing Interactive Remote Access (IRA) to a BCA or PCA, Parts 2.1-2.5 would be applicable. However, if the vendor is utilizing IRA to a PACS or EACMS, Parts 2.1-2.3 would not be applicable. This would mean no Intermediate System, no encryption, or multi-factor authentication is required. Texas RE recommends PACS and EACMS should be added.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes this is outside the scope of our SAR.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	
Document Name	
Comment	

During our discussion with the SDT SME the SME indicated that mitigation would be required for CIP-013-2 R1 and NPCC request written clarification if mitigation will be required in CIP-013-2 R1.

There is an error in the R3 moderate VSL that was carried over from the previous version. The existing text reads "…but has performed a vulnerability assessment more than 18 months ….” However, it should read "but has performed a vulnerability assessment more than 18 months, but less than 21 months ….”

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT made minimal changes between CIP-013-1 and CIP-013-2 by adding EACMS and PACS. In response to the request for written clarification, please see ERO Enterprise staff responses to questions like this on CIP-013-1, in the Frequently Asked Questions Supply Chain – Small Group Advisory Sessions (p4, with response to R1.1) document dated June 28, 2018. The team believes these responses are still applicable to CIP-013-2.

The SDT has corrected the error in CIP-010-4 R3 moderate VSL.

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

Answer	
Document Name	

Comment

Southern's comments were detailed in Questions 1-5.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see responses in questions 1-5.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
In this draft, the SDT has chosen to include all EACMS while the Commission provided the SDT with enough latitude to include only those EACMS that represent a known risk to the BES. (see Order 850, P51 where the Commission states "[We] leave it to the standard drafting team to assess the various types of EACMS and their associated levels of risks. We are confident that the standard drafting team will be able to develop modifications that include only those EACMS whose compromise by way of the cybersecurity supply chain can affect the reliable operation of high and medium impact BES Cyber Systems.") With this in mind, we encourage the SDT to reevaluate its approach and develop more targeted modification that only address the known risks associated with EACMS that perform the function of controlling electronic access.	

In addition to the concerns stated above, EEI also disagrees with the change made to proposed Reliability Standard CIP-005-7, Requirement 2, Subpart 2.5. While on the surface the change might appear to address the order, the change can be interpreted in such a way that would create an untenable dilemma. The language can be read to obligate entities to not just terminate vendor access through methods such as disabling rules within a firewall or disabling a user account for EACMS (e.g., Windows domain controller) but also to require entities to block all vendor access to the EACMS itself (i.e., install a firewall for the firewall). Unfortunately, this solution is unworkable because the new firewall would become a new EACMS obligating the entity to again install another firewall creating an endless loop of new obligations (i.e., you've entered the "hall of mirrors"). To resolve this issue, we recommend simply removing PACS and EACMS from the applicability section of Requirement R2, Subpart 2.5.

EEI also urges the SDT to develop Implementation Guidance for Industry review and comment on the proposed changes. The changes offered raise many questions on how best to develop and implement solutions that achieve effective compliance. Such guidance will help entities to better understand the proposed changes offered by the SDT.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EACMS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.

The SDT has moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.

The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting.

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
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, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	
Document Name	
Comment	

1. The IRC SRC recommends the SDT for Project 2019-03: Cyber Security Supply Chain Risks reach out to the SDT for Project 2019-02: BCSI Access Management to explore whether the vendor-related requirements currently proposed under Project 2019-02; i.e. CIP-011-3, requirement R1, part 1.4 "to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information," would be a better fit with the existing requirements under CIP-013 and, if so, discuss what would be needed to incorporate those changes into CIP-013-2. Additional support for exploring this recommendation is provided below in the form of a divergence in language between the two SDTs.

2. The IRC SRC requests the SDT collaborate with the SDT for Project 2019-02 to clarify and align the intent of CIP-013-2 requirement R1 with the *proposed* language for CIP-011-3, requirement R1, part 1.4. Currently, the language of CIP-013-2, R1, part 1.1 only requires an entity to "identify and assess cyber security risks," there is no mention of mitigation (see excerpt below):

"One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s)."

Conversely, the parallel SDT team working on Project 2019-02: BCSI Access Management has *proposed* language for CIP-011-3, requirement R1, part 1.4 that will require an entity to "identify, assess and ***mitigate*** risks in cases where vendors store Responsible Entity's BES Cyber System Information."

The IRC SRC requests the SDT collaborate with the SDT for Project 2019-02 to clarify and align the intent of this proposal with respect to mitigation:

a. Modify the language under proposed under CIP-011-3, requirement R1, part 1.4 to align with CIP-013-2, requirement R1, part 1.1 ***OR***

b. Migrate all proposed vendor-related requirements under Project 2019-02: BCSI Access Management (i.e. CIP-011-3, requirement R1, part 1.4) to Project 2019-03: Cyber Security Supply Chain Risks so that they can be addressed collectively under CIP-013-2.

The IRC SRC believes the SDT has the latitude under the SAR to undertake this consolidation per the Project Scope:

"This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to definition or standards and requirements."

Note: CAISO (segment 2, WECC region) also joins the IRC SRC in the comments provided in response to Question 6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports EEI comments on this question. In addition, upon evaluation of the addition of EACMS to CIP-005-6 R2.4 and R2.5, Xcel Energy has recognized that the requirement may limit additional controls to address the risks the requirement part is intended to address. This situation may create additional administrative burden without the consummate benefits that could be gained through policy or procedural controls. In CIP-005-6 R2.4 the Requirement states that a Responsible Entity (RE) shall “have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)”. In CIP-005-6 R2.5 the requirement states that a RE shall “have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).” Both requirements assume that RE have systems that have the capability of Vendor Remote Access (VRA) and that the RE allows for VRA if capability exists. Many entities may have systems that are not capable of VRA or do not allow for VRA in their programs. Yet the requirement as written would still force a RE to implement methods to determine VRA sessions and implement methods to disable VRA sessions. Xcel Energy believes that this issue would be eliminated by adding limited language to the Requirements that reduces the scope to only those REs that allow for VRA.	

Xcel Energy proposes adding the following or similar language to achieve this goal:

CIP-005-6 R2.4:

"Where the Responsible Entity permits vendor remote access, have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)."

CIP-005-6 R2.5:

"Where the Responsible Entity permits vendor remote access, have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access)."

Xcel Energy believes these changes can be made within the scope of the current Standard Authorization Request (SAR). In the purpose section of the SAR the Standard Drafting Team (SDT) is directed to address directives issued by FERC in Order 850 and consider NERC Staff recommendations from the NERC Staff Report. In the Cyber Security Supply Chain Risks Staff Report where they state in the Recommended Actions to Address the Risks section of CH2, P9-10 that recommended actions should "include recommendations to address EACMS risks in the process(es) used to procure BES Cyber Systems that would address identified risks specific to CIP-013-1 Requirement R1 Parts R1.2.1 through R1.2.6, as applicable, and identify existing or planned vendor mitigation strategies or procedures that address each identified risk as follows:"

· "Specific to CIP-013-1 Requirement R1 Parts R1.2.3 and R1.2.6, include recommendations relative to coordinated controls between the entity and applicable vendors associated with CIP-005-6 (Parts 2.4 and 2.5) for managing active vendor remote access sessions to and/or through EACMS cyber asset types".

In the process of addressing risk of VRA the SDT should recognize that a VRA risk is being addressed through policy or procedural controls, which current Requirement language does not allow for. If EACMS were included in the scope of the original Supply Chain project this ambiguity in requirement language could have been addressed at that time.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT has provided draft guidance around scenarios where a Responsible Entity does not permit vender remote access sessions in CIP-005-7 Implementation Guidance. Please see response to EEI in question 6.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	

David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
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 are also 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 comment. PCA’s are not in scope for this SAR.	
Monika Montez - California ISO - 2 - WECC	

Answer	
Document Name	

Comment

The IRC SRC recommends the SDT for Project 2019-03: Cyber Security Supply Chain Risks reach out to the SDT for Project 2019-02: BCSI Access Management to explore whether the vendor-related requirements currently proposed under Project 2019-02; i.e. CIP-011-3, requirement R1, part 1.4 "to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information," would be a better fit with the existing requirements under CIP-013 and, if so, discuss what would be needed to incorporate those changes into CIP-013-2. Additional support for exploring this recommendation is provided below in the form of a divergence in language between the two SDTs.

During discussion with a member of the SDT, the member indicated mitigation would be required for CIP-013-2 requirement R1. Currently, the language of CIP-013-2, R1, part 1.1 only requires an entity to "identify and assess cyber security risks" and not mitigate them as detailed below.

"One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s)."

That said, the parallel SDT team working on Project 2019-02: BCSI Access Management has *proposed* language for CIP-011-3, requirement R1, part 1.4 that will require an entity to "identify, assess and ***mitigate*** risks" as detailed below:

"Processes to identify, assess, and ***mitigate*** risks in cases where vendors store Responsible Entity's BES Cyber System Information."

If the intent of this proposal is to require mitigation for ***all*** assets under CIP-013, requirement R1, part 1.1, the IRC SRC requests the SDT to:

- Modify the language under CIP-013-2, requirement R1, part 1.1 to mirror the language proposed under CIP-011-3, requirement R1, part 1.4 ***OR***

Migrate all proposed vendor-related requirements under Project 2019-02; i.e. CIP-011-3, requirement R1, part 1.4, to Project 2019-03: Cyber Security Supply Chain Risks so that they can be addressed collectively under CIP-013-2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	
Comment	
To prevent possible confusion we suggest that all modifications proposed for CIP-005 and CIP-010 should be documented in one CIP standard (CIP-013).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Fundamentally, CIP-013 is a planning horizon standard to manage cyber security risks throughout the supply chain up to installation whereas the proposed requirements to CIP-005 and CIP-010 apply to applicable systems that are in-service in the operations horizons.	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	

1. The NERC SAR for this order is poorly written and inaccurate at best. The intent of the SAR is to communicate the ask, the specifics around what is required, and citations for the basis. Recommend revising the SAT to include the specific FERC Order and NERC technical paper requirements and recommendations. 2. Consider revising CIP-002 to identify all different Cyber System and Cyber Asset types and their ability to be accessed locally and remotely (physical and electronic). Distinguish between EACMS and PACS which provide preventive and detective controls and identify internal controls which meet the audit requirements and are agreeable to industry	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The time period to comment on the SAR expired on 8/1/2019. The supply chain standards only consist of CIP-005, CIP-010 and CIP-013. Therefore changes to CIP-002 are not possible for the 2019-03 SDT.	
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 response.	
Daniel Gacek - Exelon - 1	

Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	

Comment

PG&E agrees with the EEI input on Question 6 regarding the modification to CIP-005-7, Requirement R2, Part 2.5 creating an untenable dilemma based on how it could be interpreted. This is based on the EEI comment of:

"The language can be read to obligate entities to not just terminate vendor access through methods such as disabling rules within a firewall or disabling a user account for EACMS (e.g., Windows domain controller) but also to require entities to block all vendor access to the EACMS itself (i.e., install a firewall for the firewall)."

EEI additionally indicated that if entities are required to block all access to the EACMS by installing a separate firewall, the newly installed firewall would be an EACMS which would then need to have another firewall installed creating an endless loop of new obligations.

While the EEI recommendation indicates to remove EACMS from the Applicability Section of Requirement R2, Part 2.5, PG&E believes this would result in the modification not meeting FERC's directive in Order 850.

PG&E recommends the Requirement language be modified to indicate the endless loop condition is not the intended purpose of the modification, or guidance be created which clearly indicates it is not the intended purpose of the Requirement. The preferred solution is Requirement language since Audit Teams are not bound to the wording in guidance.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see response to EEI in question 6. The SDT has moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	
Document Name	

Comment	
FirstEnergy urges the SDT to develop Implementation Guidance for Industry review and comment on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	
Document Name	
Comment	
CEHE supports the additional comments as submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI for question 6.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	

During our discussion with the SDT SME the SME indicated that mitigation would be required for CIP-013-2 R1 and TFIST request written clarification if mitigation will be required in CIP-013-2 R1. There is an error in the R3 moderate VSL that was carried over from the previous version. The existing text reads "…but has performed a vulnerability assessment more than 18 months …." However, it should read "but has performed a vulnerability assessment more than 18 months, but less than 21 months …."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT made minimal changes between CIP-013-1 and CIP-013-2 by adding EACMS and PACS. In response to the request for written clarification, please see ERO Enterprise staff responses to questions like this on CIP-013-1, in the Frequently Asked Questions Supply Chain – Small Group Advisory Sessions (p4, with response to R1.1) document dated June 28, 2018. The team believes these responses are still applicable to CIP-013-2. The SDT has corrected the error in CIP-010-4 R3 moderate VSL.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports RSC comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT made minimal changes between CIP-013-1 and CIP-013-2 by adding EACMS and PACS. In response to the request for written clarification, please see ERO Enterprise staff responses to questions like this on CIP-013-1, in the Frequently Asked Questions Supply Chain – Small Group Advisory Sessions (p4, with response to R1.1) document dated June 28, 2018. The team believes these responses are still applicable to CIP-013-2. The SDT has corrected the error in CIP-010-4 R3 moderate VSL.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
Why are Protected Cyber Asset (PCA) or Protected Cyber System (PCS) per CIP [Definitions: Project 2016-02 Modifications to CIP Standards] not considered; given that the “impact rating of the PCA [or PCS] is equal to the highest rated BCS in the same ESP?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. PCA’s are not in scope for this SAR.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	
Document Name	
Comment	
Comments:	

1.) Recommend the SDT for Project 2019-03: Cyber Security Supply Chain Risks reach out to the SDT for Project 2019-02: BCSI Access Management to explore whether the vendor-related requirements currently proposed under Project 2019-02, i.e. CIP-011-3, requirement R1, part 1.4, “to identify, assess, and mitigate risks in cases where vendors store Responsible Entity’s BES Cyber System Information,” would be a better fit with the existing requirements under CIP-013 and, if so, discuss what would be needed to incorporate those changes into CIP-013-2. Additional support for exploring this recommendation is provided below, showing the divergence in language between the two SDTs.

2.) A SDT member indicated in conversation that mitigation would be required for CIP-013-2 requirement R1. The current language of CIP-013-2, R1, part 1.1, only requires an entity to “identify and assess cyber security risks;” there is no mention of mitigation.

Conversely, the parallel SDT team working on Project 2019-02: BCSI Access Management has proposed language for CIP-011-3, requirement R1, part 1.4, that will require an entity to

implement one or more documented information protection program(s) including “Processes to identify, assess, and mitigate risks in cases where vendors store Responsible Entity’s BES Cyber System Information.”

We request the SDT, in order to avoid duplication of requirements across multiple standards, to collaborate with the SDT for Project 2019-02 to either:

- Migrate all vendor-related requirements currently proposed under CIP-011-3, R1, Part 1.4 to CIP-013-2,

OR

- Drop any plans to introduce mitigation in CIP-011-3, R1, Part 1.4 and defer to the language in the existing, similar requirement under CIP-013-1, R1, Part 1.1.

We believe the SDT has the latitude under the SAR to undertake this consolidation per the Project Scope:

“This project will address the directives issued by FERC in Order No. 850. This project will also consider NERC staff recommendation from the Supply Chain Report. This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to definition or standards and requirements.”

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;

Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy suggests the following: Current CIP standards don't require entity to go beyond ESP boundary to monitor vendor remote access. Since all EACMS and PACS system don't reside within an ESP, the focus of this standard will shift beyond ESP boundary, where will be required to monitor and possibly terminate such access before such traffic even gets to ESP firewall. Duke Energy believes only EACMS or PACS devices that reside within an ESP should be the focus of this standard, so original intention of CIP-005 protection at the ESP level doesn't get derailed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. FERC Order 850 and the NERC Supply Chain Report did not specify only certain EACMS and PACS should be protected but all EACMS and PACS should be protected. The SDT drafted the standards to meet those requirements.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	
Document Name	
Comment	

We suggest moving revised CIP-011-2 R1.4 to CIP-013 R1.1 to address BCSI cloud services provider’s risks since it really belongs to the supply chain risk management.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	
Document Name	
Comment	
FERC/NERC should be vetting Vendors and creating a list for us. Similar to Underwriter Labs (UL) reviewing, vetting, and testing equipment, then stamping it for appropriate use.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the SDT has passed this comment along to NERC compliance. CIP-013 including industry guidance for compliance with CIP-013 provides flexibility to use an independent assessment or third-party accreditation when vetting vendors.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	
Comment	

I feel FERC/NERC should be vetting Vendors and creating a list for us. Similar to Underwriter Labs (UL) reviewing, vetting, and testing equipment, then stamping it for appropriate use.

Likes 0	
Dislikes 0	

Response

Thank you for your comment, the SDT has passed this comment along to NERC compliance. CIP-013 including industry guidance for compliance with CIP-013 provides flexibility to use an independent assessment or third-party accreditation when vetting vendors.

sean erickson - Western Area Power Administration - 1

Answer	
Document Name	

Comment

1. The NERC SAR for this order is poorly written please revise to include the FERC Order and NERC technical paper requirements

2. Consider revising CIP-002 to identify all different Cyber System and Cyber Asset types and their ability to be accessed locally and remotely (physical and electronic). Distinguish between EACMS and PACS which provide preventive and detective controls and identify internal controls which meet the audit requirements and are agreeable to industry

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The time period to comment on the SAR expired on 8/1/2019.

The supply chain standards only consist of CIP-005, CIP-010 and CIP-013. Therefore changes to CIP-002 are not possible for the 2019-03 SDT.

Marty Hostler - Northern California Power Agency - 5

Answer	
Document Name	
Comment	
I feel FERC/NERC should be vetting Vendors and creating a list for us. Similar to Underwriter Labs (UL) reviewing, vetting, and testing equipment, then stamping it for appropriate use.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the SDT has passed this comment along to NERC compliance. CIP-013 including industry guidance for compliance with CIP-013 provides flexibility to use an independent assessment or third-party accreditation when vetting vendors.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	
Document Name	

Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Wayne Guttormson - SaskPower - 1	
Answer	
Document Name	
Comment	
Support the MRO comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response to MRO in question 6.	

End of Report