Comment Report

Project Name:	Project 2019-03 Cyber Security Supply Chain Risks
Comment Period Start Date:	7/2/2019
Comment Period End Date:	8/1/2019
Associated Ballots:	

There were 29 sets of responses, including comments from approximately 80 different people from approximately 61 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

2. Provide any additional comments for the SAR drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Santee Cooper	Chris Wagner	1,3,5,6		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
Public Utility District No. 1 of Chelan County	Davis Jelusich	1,3,5,6		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Jennifer Bray	Arizona Electric Power Cooperative	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
Duke Energy		1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC

	Katherine Street				Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Adrianne Collins	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
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
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Michael Jones	National Grid	3	NPCC

Sean Cavote	PSEG	4	NPCC
Kathleen Goodman	ISO-NE	2	NPCC
David Kiguel	Independent	NA - Not Applicable	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Gregory Campoli	New York Independent System Operator	2	NPCC
Laura McLeod	NB Power Corporation	5	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
John Hastings	National Grid	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
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
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

Comments: GTC encourages limiting the scope of the SAR to address the directive issued by FERC in order 850 due to the following basis:

· Entities have not yet fully implemented the CIP-013 programs which apply to high and medium impact BES Cyber Systems; and therefore such addition at this immature stage in the implementation cycle could over complicate and disrupt the focused attention necessary to fully implement in its current state.

· The additional undirected scope could cause opposition by industry and thus delays in NERC meeting FERC's Standard revision submittal deadline "24 months from the effective date of Order No. 850".

· The current version of CIP-013-1 already requires entities to identify and assess risks of vendor services for installing BES Cyber Assets (equipment/software). Such service type vendors that can perform installation services at high or medium impact locations are required to have "CIP" physical access via each entities CIP program. Vendors that do not have physical access (escorted visitor access) can also be identified and assessed accordingly by each entity. Therefore, the physical access component will be assessed and addressed by each entity as part of implementation of CIP-013-1 R1.1 already.

· PACs components installed at physical security perimeters housing BES Cyber Systems are video monitored/protected under the CIP program. Any compromise at the device level performed in the cyber realm must ultimately be accompanied by physical presence in order to gain access inside the physical security perimeter. Unauthorized physical access would be recognized and acted upon in very short fashion even if material was compromised at the manufacturer supplier "supply chain" level. Therefore, GTC sees the addition of PACS in CIP-013-2 as premature at this time and adequately monitored (and risk managed) by CIP programs.

For the various reasons above, GTC encourages NERC to be patient and let entities implement CIP-013 programs which will apply to high/medium impact BES Cyber Systems and EACMS before attempting to expand the scope at such an early stage in the implementation and audit cycle.

Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	

GSOC encourages limiting the scope of the SAR to address the directive issued by FERC in order 850 due to the following basis:

- Entities have not yet fully implemented the CIP-013 programs which apply to high and medium impact BES Cyber Systems; and therefore such addition at this stage in the implementation cycle could over complicate and disrupt the focused attention necessary to fully implement in its current state.
- The additional undirected scope could cause opposition by industry and thus delay NERC meeting FERC's Standard revision submittal deadline "24 months from the effective date of Order No. 850".

For the various reasons above, GSOC encourages NERC to be patient and let entities implement CIP-013 programs which will apply to high/medium impact BES Cyber Systems and EACMS before attempting to expand the scope at such an early stage in the implementation and audit cycle.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3,5

Answer	Yes
Document Name	

Comment

AEP agrees with the proposed scope as described in the SAR primarily because the exclusion of the EACMS and PACs could result in unauthorized access to the BES. These systems have also been found to be a gateway to other systems. Even if only the EACMS and PACs systems were compromised it could result in unauthorized physical and logical access to protected systems.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the Standard Authorization Request (SAR) modifications to include Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) involved with medium and high impact BES Cyber Systems (BCS), excluding those devices which handle only monitoring and/or logging capabilities.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company supports including EAMCS of the proposed Supply Chain Standard that apply to access control and exclude monitoring and logging functions. Southern also supports possibly changing the complete definition of EACMS that would apply to the this standard and other CIP Standards and recommends the SDT to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System. Southern does however disagree with NERC including PACS assets into the scope of CIP-013 Supply Chain Standard. There is not a clear path to define who could or would be the potential vendor of PACS assets; the third party reseller or the manufacturer. The company who ultimately supplies Southern with the assets may not be the party who purchases the assets on behalf of Southern as in the case with controller panels. PACS workstations which could be Dell machines would not be purchased directly from Dell but from a reseller who provides for all of Southern, but not necessarily for PACS specifically. The risk based approach for PACS assets would be very limited in scope.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
None	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO appreciates the efforts of CIPC Supply Chain Working Group (SCWG) in drafting these guidelines. IESO supports the comments submitted by NPCC.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	

FERC Order No. 850 directed modifications to the supply chain risk management Reliability Standards to include EACMS. Paragraph 6 stated that more study is necessary to determine the impact of PACS and PCAs.

NERC published its study and recommendations in the May 17, 2019, Cyber Security Supply Chain Risks Staff Report and Recommended Actions. That report recommends addressing PACS in the Cyber Security Supply Chain standards, but not including PCAs at this time.

The scope of this SAR is consistent with the FERC order and the findings of the NERC study.

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

Although addressing PACS is not a directive from FERC, it seems prudent to expand the scope of the SAR beyond the FERC order to include PACS, since the standard is being modified.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

- PAC agrees with the Standard Authorization Request (SAR) modifications to include Electronic Access Control or Monitoring Systems (EACMS) specifically involved with medium and high impact BES Cyber Systems (BCS), excluding those devices which handle only monitoring and/or logging capabilities
- PAC agrees with including Physical Access Control Systems (PACS) that provide physical access control, excluding alarming and logging, to high and medium impact BES Cyber Systems, primarily because the exclusion of the EACMS and PACs could result in unauthorized access to the BES

Likes 0	
Dislikes 0	

Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
NERC is recommending addressing PACS as part of this SAR. NERC needs to consider the challenges related to supply chain for end-point PACS such as control panels in fire control rooms, communication facilities, etc... Many transmission and generation entities rely on large and small contract companies to maintain these end-point control panel PACS, and attempting to identify chipset software and/or operating system suppliers or manufacturers will be challenging and in some cases not feasible. In addition, depending on an entities physical and electronic protections of PACS, the risk of Supply Chain outweighs the benefit. NERC may desire to consider compensating controls options within Supply Chain for PACS which can be verified by the contract or vendor support companies.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	

Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NVE agrees with the SAR on inclusion of EACMS and PACS that are associated with High and Medium Impact BCS.	
Likes 0	
Dislikes 0	
Response	
Nick Batty - Keys Energy Services - 4	
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	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Zwergel - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katherine Street - Duke Energy - 1,3,5,6 - SERC,RF, Group Name Duke Energy	
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

2. Provide any additional comments for the SAR drafting team to consider, if desired.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
NVE provides the following recommendations for the SDT: • Language needs to be consistent and take the SAR Scope to include acknowledging the need for on-going coordination between the Project 2016-02 and Project 2019-03 SDTs • When revising CIP-013-1, keep in mind the exclusion of “locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers” from the PACS definition per the NERC Glossary.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	
Document Name	
Comment	
GSOC recommends adding a review of the definition(s) of EACMS, PACS, and to define new term(s) accordingly to exclude monitoring and logging from the addition of EACMSs and/or to exclude alarming/alerting and logging from the PACs definition as part of the scope of this SAR.	

Specifically, this project could consider separate definitions to clarify and distinguish access/control type systems such as Electronic Access Control Systems (EACS) and PACS, from alarming/logging type systems such as Electronic Alarming, Monitoring or Logging Systems (EAMLS) as separate NERC defined terms. This clarity would appropriately categorize new alarming/alerting/logging “only” type systems as BESCI repositories as well as distinguish access/control type systems in an unbundled manner.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	
Document Name	

Comment

GTC recommends to add a review of the definition(s) of EACMS, PACS, and to define new term(s) accordingly to exclude monitoring and logging from the addition of EACMSs and/or to exclude alarming/alerting and logging from the PACs definition as part of the scope of this SAR.

Specifically, this project could consider separate definitions to clarify and distinguish access/control type systems such as Electronic Access Control Systems (EACS) and PACS, from alarming/logging type systems such as Electronic Alarming, Monitoring or Logging Systems (EAMLS) as separate NERC defined terms. This clarity would appropriately categorize new alarming/alerting/logging “only” type systems as BESCI repositories.

Likes 0	
Dislikes 0	

Response

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	
Comment	

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

Yes

No

Comments:

- PAC agrees with the Standard Authorization Request (SAR) modifications to include Electronic Access Control or Monitoring Systems (EACMS) specifically involved with medium and high impact BES Cyber Systems (BCS), excluding those devices which handle only monitoring and/or logging capabilities
- PAC agrees with including Physical Access Control Systems (PACS) that provide physical access control, excluding alarming and logging, to high and medium impact BES Cyber Systems, primarily because the exclusion of the EACMS and PACs could result in unauthorized access to the BES

1. Provide any additional comments for the SAR drafting team to consider, if desired.

Comments:

- “R1.1 should be read as “The plan(s) shall include one or more process(es) for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services …” followed by the rest of R1.1.”
- There is a missing component: Mitigate:
    - This is the second word in the “Purpose” of the Standard, but it is not listed anywhere else in the entire Standard – basically this leaves an action intended, but not stated to perform
- If low impact BCS are included in the scope of CIP-013, PAC recommends the standard allow entities to make a risk-based decision to purchase and implement a product in the absence of that product’s vendor being able to meet the entity’s requirements (e.g., R1.2.1 through R1.2.6)
- Will CIP Exceptional Circumstances be considered for Cyber Assets and software procured for emergencies?

- Language needs to be consistent and take the SAR Scope to include acknowledging the need for on-going coordination between the Project 2016-02 and Project 2019-03 SDTs
- When revising CIP-013-1, keep in mind the exclusion of “locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers” from the PACS definition per the NERC Glossary

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Thank you for the opportunity to comment

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

When revising the supply chain risk management Reliability Standards, keep in mind the exclusion of “locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers” from PACSs per the NERC Glossary definition.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	
Document Name	

Comment
Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment
The Project 2016-02 SDT is strongly considering changes to the definition aand classification of EACMS to more fully address the realities and technical concerns of “access control” vs “access monitoring” systems and the need to consider 3rd party services for best practices in enterprise monitoring. In light of the proposed separation of EACMS into EAMS and EACS, the directive to modify within 24 months of Order 850 could have significant impact on any effort to evaluate the supply chain for products and services that the RE does not have on-premises or that may be under contractual agreement rather than direct control.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment
If approved, the following is provided as feedback to the NERC SDT that will be addressing the SAR: Southern Company suggests the SDT consider modifying the glossary definition of EACMS and to revise the Supply Chain Reliability Standards to include: (i) EACMSs, specifically those systems that provide electronic access control (**excluding monitoring and logging**) to high and medium impact BES Cyber Systems; and (ii)PACSs that provide physical access control (**excluding alarming and logging**) to high and medium impact BES Cyber Systems, if PACS is to be added.

Likes 0	
Dislikes 0	

Response

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

Comment

Reclamation recommends CIP-013 be revised to allow entities to implement a single process for procuring products and services associated with all impact levels of their BCS as well as all applicable systems (EACMS, PACS, PCAs, etc.). To achieve this, Reclamation recommends allowing entities to apply CIP-013-1 procurement protections to their low impact systems. Having the standard only apply to high and medium impact BCSs and their applicable systems could introduce risk through the unmanaged CIP-013-1 procurement portions of those systems that also support low impact BCS.

If low impact BCS are included in the scope of CIP-013, Reclamation recommends the standard allow entities to make a risk-based decision to purchase and implement a product in the absence of that product's vendor being able to meet the entity's requirements (e.g., R1.2.1 through R1.2.6).

Reclamation recommends the objectives for ensuring supply chain security throughout the procurement process not be left to choice as this will cause inconsistency across the industry. Therefore, Reclamation recommends NERC investigate existing supply chain risk management standards (e.g., National Institute of Standards and Technology, Federal Acquisition Supply Chain Security Act of 2018, and Section 889 of the National Defense Authorization Act for Fiscal Year 2019) and align CIP-013-1 with those requirements.

Reclamation recommends the revised CIP-013 standard include procurement protections of routable components for low impact BCSs, EACMS, PACS, and PCAs. The SAR should include procurement protections for EACMS, PACS, PCAs commensurate with the highest level of BES Cyber System managed by each PACS.

Finally, Reclamation recommends a 24-month implementation period for entities to comply with the revised high and medium impact portions of CIP-013 and a 48-month implementation period for entities to comply with any new low impact requirements.

Likes 0	
Dislikes 0	

Response

Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	
Document Name	

Comment

Would associated EACMS and PACS be brought in-scope for CIP-005-6 R2 and CIP-010-3 R1.6? Please address exceptions for open source or free software not provided by the vendor but needed for operations (Putty, Wireshark, etc.). Please address whether the standard necessitates an asset management system to link Cyber Assets and software to the contract they are procured under. Will CIP Exceptional Circumstances be considered for Cyber Assets and software procured for emergencies?

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	
Document Name	
Comment	
Dominion Energy agrees with EEI's additional comments, specifically: 1. That NERC provide a link to the May 17, 2019, Cyber Security Supply Chain Risks Staff Report and Recommended Actions within the SAR since this report is being used to set the boundaries that will be used by the SDT when addressing modifications to PACSs. While the report is mentioned within the SAR, we believe tighter linkage to this report would be beneficial, and 2. That language be added to the SAR Scope to include acknowledging the need for on-going coordination between the Project 2016-02 and Project 2019-03 SDTs. Given the overlapping project efforts, we believe it is important that both SDTs remain aligned throughout the life of each project.	
Likes 0	
Dislikes 0	
Response	

Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	
Document Name	
Comment	
PG&E provides no additional comments.	
Likes 0	
Dislikes 0	

Response
Leanna Lamatrice - AEP - 3,5
Answer	
Document Name	
Comment
The exclusion of these systems was discussed heavily during the drafting of the standards. It is AEP's belief that if these systems are not included in the standard we are leaving a significant opening for an attacker.
Likes 0	
Dislikes 0	
Response
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper
Answer	
Document Name	
Comment
No comments.
Likes 0	
Dislikes 0	
Response