Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization Updates for CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, and Associated Definitions
Comment Period Start Date:	11/2/2018
Comment Period End Date:	12/18/2018
Associated Ballots:	

There were 76 sets of responses, including comments from approximately 199 different people from approximately 132 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The proposed BCS definition no longer relies on the term Cyber Asset. The SDT asserts that the proposed BES Cyber System definition describes the BCS adequately without the use of the word "programmable" in the definition. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT asserts that the proposed Cyber Asset definition provides clarity around virtual hardware. (Cyber Assets revised definition: Programmable electronic devices, including the physical or virtual hardware, software, and data in those devices.) Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. The SDT asserts that the term Cyber Asset should continue to be used within the NERC Glossary of Terms for: Removable Media and Transient Cyber Asset. Due to the nature of that type of hardware, these devices do not lend themselves to the systems approach. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicability for the monitoring portion to allow third party monitoring systems. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

5. The SDT realized through the process of splitting EACMS that the same considerations apply to PACS, which will allow changes within the applicability for alerting and logging (PAMS is not reflected within the applicability section at this time). The SDT is considering splitting the PACS term into PACS and PAMS to allow third party monitoring or event correlation to be performed without carrying the PACS classification. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

6. The SDT is proposing to move away from the more prescriptive ESP/EAP model to logical isolation through the higher level objectives provided by the BES Cyber System concept and its Logical Isolation Zone. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

7. The SDT is considering taking qualitative language out of the Intermediate System definition and using it to clarify requirements. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

8. The SDT is considering changes to the ERC and IRA definitions to address V5TAG issues (see the CIP-005 Technical Rationale document for detailed information). ERC will have conforming changes only and will continue its use as a scoping mechanism. The proposed modifications to IRA will apply to certain non-routable to routable protocol conversion scenarios. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

9. To the extent possible, the SDT intends its modifications to permit approaches to compliance that are "backwards compatible" with compliance approaches within the currently approved versions of the CIP standards. (Notable exceptions include CIP-005 R3, CIP-007 R2, and Secure Configurations – CIP-010). Do you agree the modifications are backwards compatible? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

10. The SDT has not yet determined a proposed timeframe to include in the Implementation Plan. How long would you as an entity need to implement the proposed modifications? Please provide your implementation timeframe and justification for why that amount of time would be needed.

11. The SDT is proposing conforming modifications to CIP-004. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. Modifications related to CIP Exceptional Circumstances

b. Use of newly proposed terms EACS and EAMS in the Applicable Systems column

c. Addition of PCS to the Applicable System column for Parts in CIP-004 to mitigate security risks associated with individuals not needing authorization or PRAs when granted access to systems inside the Logical Isolation Zone

12. The SDT is proposing modifications to CIP-005 (see the CIP-005 Technical Rationale document for detailed information). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The replacement of the ESP concept with Logical Isolation Zone (LIZ).

b. Is the backward compatibility clear as existing ESPs and EAPs move to the new LIZ concept?

c. The addition of the 4.2.3.3 exemption in the standard along with the addition of Requirement part R1.2 to address the V5TAG concern of "Super ESPs" or single networks within or between BES Cyber Systems that span more than one geographic location.

d. As differing forms of shared infrastructure come into play with virtualization, Requirement R3 has been added to include the management plane and its isolation controls as a part of the CIP standards. Is this concept clearly and widely understood?

13. The SDT is proposing conforming modifications to CIP-006. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. Modifications related to CIP Exceptional Circumstances

b. Use of newly proposed term EACS in the Applicable Systems column

14. The SDT is proposing modifications to CIP-007 (see the CIP-007 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-007. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?

b. The SDT is proposing the security objective in CIP-007 R1, "to mitigate the risk posed by uncontrolled logical and physical connectivity". Do you agree that the modifications to CIP-007 R1 Part 1.1 fulfill this security objective for systems where connectivity is not limited to TCP/IP port service combinations, as in virtualized systems and SAN based storage?

c. Do you agree that the modifications to CIP-007 R1 Part 1.1 add necessary flexibility to fulfill the security objective of CIP-007 R1 for virtualized systems and provides a degree of future proofing?

15. The SDT is proposing modifications to CIP-010 (see the CIP-010 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-010. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?

b. The SDT is proposing to modify the referenced baseline configuration from CIP-010-3 R1 Part 1.1 to a 'Secure Configuration' which is made up of the implemented controls that fulfill requirements within CIP-005 and CIP-007. Do you agree that this set of controls supports managing change under CIP-010 R1 Part 1.1?

c. The SDT is proposing to modify the current CIP-007 R2 requirements and move them to CIP-010 R3. The SDT believes that the software vulnerability management found within this set of requirements fits logically within the security objective of CIP-010 R3 "to mitigate the risk posed by system vulnerabilities" and has moved it there. Do you agree?

d. The SDT is proposing CIP-010 R3 Parts 3.5 and 3.6 to replace the current CIP-007 R2 Parts 2.1 – 2.4. Do you agree that the proposed CIP-010 R3 Parts 3.5 and 3.6 offer the additional flexibility needed when implementing virtualized systems that can be dormant for a period, and for which security patches have become available?

16. Provide any additional comments for the SDT 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
BC Hydro and Power Authority	Adrian Andreoiu	1,3,5	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
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
					Travis Bryan	Santee Cooper	1,3,5,6	SERC
					Shedrick Snider	Santee Cooper	1,3,5,6	SERC
					Wanda Williams	Santee Cooper	1,3,5,6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO

					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
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
PPL - Louisville Gas and Electric Co.	Devin Shines	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
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
Great Plains Energy - Kansas City	Douglas Webb	1,3,5,6	MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO

Power and Light Co.								
Lincoln Electric System	Eric Ruskamp	1,3,5,6		LES	Eric Ruskamp	Lincoln Electric System	6	MRO
					Dan Pudenz	Lincoln Electric System	1	MRO
					Jason Fortik	Lincoln Electric System	3	MRO
					Kayleigh Wilkerson	Lincoln Electric System	5	MRO
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
ACES Power Marketing	Jodirah Green	6	NA - Not Applicable	ACES Standard Collaborations	Eric Jensen	Arizona Electric Power Cooperative, Inc	1	WECC
					Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Greg Froehling	Rayburn Country Electric Cooperative, Inc.	3,6	Texas RE

					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Amber Skillern	East Kentucky Power Cooperative	1,3	SERC
					Ginger Mercier	Prairie Power, Inc.	1,3	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Southwest Power Pool, Inc. (RTO)	Kimberly Van Brimer	2	MRO	SPP Member Group	Matt Harward	SPP	2	MRO
					Louis Guidry	Cleco	1,3,5,6	SERC
					Joe Gatten	Xcelenergy	1,3,5,6	MRO
Manitoba Hydro	Mike Smith	1,3,5,6		Manitoba Hydro	Yuguang Xiao	Manitoba Hydro	5	MRO
					Karim Abdel-Hadi	Manitoba Hydro	3	MRO
					Blair Mukanik	Manitoba Hydro	6	MRO
					Mike Smith	Manitoba Hydro	1	MRO
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC

Lakeland Electric	Patricia Boody	1,3,5,6		Lakeland CIP	Jim Howard	Lakeland Electric	5	FRCC
					Larry Watt	Lakeland Electric	1	FRCC
					Paul Shipps	Lakeland Electric	6	FRCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and NYPA	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
					Caroline Dupuis	Hydro Quebec	1	NPCC

					Chantal Mazza	Hydro Quebec	2	NPCC
					Michael Forte	Con Edison	1	NPCC
					Laura McLeod	NB Power Corporation	5	NPCC
					Nick	Kowalczyk	1	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					John Hastings	National Grid	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Sofia Gadea-Omelchenko	Con Edison	5	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
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
PSEG	Sean Cavote	1,3,5,6	FRCC,NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - PSEG Energy Resources and Trade LLC	6	RF

					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co.	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF
Lower Colorado River Authority	Teresa Cantwell	1,5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Associated Electric Cooperative, Inc.	Todd Bennett	1,3,5,6		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri	1	SERC

						Electric Power Cooperative		
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The proposed BCS definition no longer relies on the term Cyber Asset. The SDT asserts that the proposed BES Cyber System definition describes the BCS adequately without the use of the word "programmable" in the definition. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Greg Davis - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	

Comment

It's clear, but concern about how it will be audited. Concerns that there is not clear tie to an impact to the BES and its replaced with only the impact to a BES Facility.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	

Comment

It's clear, but concern about how it will be audited. Concerns that there is not clear tie to an impact to the BES and its replaced with only the impact to a BES Facility.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

IESO agrees with the new BCS definition. While this change may add additional assets/devices into the CIP program (via re-evalutation of CIP-002), the controls being used should remain the same.

Likes 0	

Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Yes, however adding the 15-minute requirement to BCS might change the composition of our Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Yes, however adding the 15-minute requirement to BCS might change the composition of our Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA. Please see our response to Question 16, below, for a summary of our comments and position regarding the changes and approached proposed herein.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	

Comment

APPA does not believe the removal of “programmable” adequately scopes the applicable device types with the current definition. APPA believes that the new definition would include devices that have been previously excluded, such as electro-mechanical relays, since “any combination of” would include hardware only, and there is no scope placed on the hardware to eliminate these devices.

In any case, because “programmable” remains in the legacy definition of “cyber asset,” the issue about its meaning—to the degree that remains an issue—has not been eliminated.

Additionally, APPA does not believe the proposed BES Cyber System definition describes the BCS appropriately. The new definition is attempting to combine many definitions into one. Public power recommends using the language below:

A BES Cyber System includes any combination of programmable hardware (including virtual hardware), software (including application virtualization), and data, where:

1. It/they performs one or more reliability tasks; and

2. If rendered unavailable, degraded, or misused, the situation would result in adverse impact to one or more BES Facilities within 15 minutes. Redundancy is not a factor, in the sense of considering the activation of different, redundant BES Cyber Systems.

The language “regardless of redundancy,” as used in the proposed definition, is unclear. Does “regardless of redundancy” apply to all items (hardware, software, and data)? It seems that the redundancy being introduced is intended to address the BES Cyber Asset definition, but the language structure makes this difficult to decipher. We understand that redundancy in determining systems is based on the language in CIP-002-5.1a as it relates to Real-Time Operations:

“This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.” In this regard, revisions to the core BCS definition will require some Entities to re-work their CIP-002-5.1a process to address the Real-time Operations decision at a different point in the process to identify BES Cyber Systems.

The recommended revised definition above attempts to incorporate these concepts.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

The current BCS definition has the potential to increase the scope / applicability of the CIP standards. The BCS definition should include a reference to Cyber Asset definitions, and further define what is meant by hardware, software, data, etc. As currently written, it seems “hardware” that do not satisfy the definition of Cyber Asset could be brought in under the BCS definition.

In addition, any changes to existing terminology or definitions should provide a security benefit considering the extent of administrative changes that will be required to implement these changes (policies, procedures, tools, asset management systems, device labeling, updated training materials, implementing staff training, etc.). It seems the current proposed change does not provide a security benefit.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). This proposed change would require entities to re-evaluate what is in scope under CIP-002 and could cause non-programmable devices to be included. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs. SMEC is concerned that this magnitude of change to the CIP standards would be too disruptive to non-virtualization compliance.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes that for the sake of avoiding arguments during audits, the word, “programmable” should be retained. Suggest rewording: “A programmable combination of physical and/or virtual hardware, software and data, performing or supporting one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes. Redundancy shall not be considered when identifying BES Cyber Systems.”

Likes 0	

Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	No
Document Name	

Comment
We believe the the new definition of BES Cyber System should contain the term Cyber Asset, like: "Any combination of Cyber Assets, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes." Additionally, we believe the new definition, without the use of "programmable" will bring into scope electronic devices that are not capable of being updated and have no means to update the software or firmware within them (not field updateable). These devices currently do not meet the “programmable” electronic device definition and are thus out of scope for NERC CIP.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	

Comment
The proposed definition of BCS does not address the issues and interpretations that surfaced by not having a definition of programmable.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	

Comment
ITC is in agreement with the comments submitted by EEI:

"EEI does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). While we understand the SDT's desire to move from the current asset focused model to a systems approach, the changes being proposed within the body of revised and retired definitions appears to go well beyond what we understand was intended within the currently approved SAR.

EEI believes that the SDT should retain the defined terms "BES Cyber Assets (BCA)" and BES Cyber System (BCS) as currently written. We also believe that given the proposed revisions made to the term "Cyber Asset," which clarify that physical or virtual hardware, software and data are allowed, obviates the need to revise the other definitions."

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Some concern that "Any combination of hardware.." with out programmable could lead to more confusion about what specific devices are or are not in-scope.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

Exelon does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). While we understand the SDT's desire to move from the current device-focused model to a systems approach, the changes being proposed involve fundamental definitions and appear to go well beyond what we understand was intended within the currently approved SAR. The proposed change represents a major overhaul of the CIP Standards, including impacts on CIP-002 methodologies, assessment methods, and many current CIP Program processes and procedures. These changes would be better addressed in a separate and comprehensive major CIP version upgrade effort.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	No
Document Name	
Comment	
Some concern that "Any combination of hardware.." with out programmable could lead to more confusion about what specific devices are or are not in-scope.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
Covering all items without consideration of the difference between programmable and non-programmable devices introduces significant complications for physical security and for configuration management. Should an auditor independently determine that communications cabling, electrical wiring, or non-programmable devices such as electro-mechanical relays are part of the system, the scope of CIP-006 could grow drastically. This could have a tremendous impact on medium impact generation assets. While "programmable" or a suitable variation of the term is needed, the issues with the current non-definition of programmable need to be addressed. The definition is based on programmable, the various types of programmability needs to be addressed: (1) Remotely programmable; (2) requires physical access and interruption of operation to change device programming; Electromechanical devices (including devices such as electromechanicable breakers and physical hardware such as communications cabling and electrical wiring). .	

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	No
Document Name	

Comment

CHPD disagrees with the removal of Cyber Asset from the definition. The new language will expand the current scope of the definition by bringing any electro-mechanical BES device into scope due to “Any combination…” language and the lack of a tie to the “Programmable” term defined in the Cyber Asset definition.

CHPD suggests using the new Cyber Asset definition (already scopes virtual systems) with the following BES Cyber System definition:

“A combination of one or more Cyber Assets performing one or more reliability tasks, including redundant members that support a reliability task, that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.”

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). While we understand the SDT’s desire to move from the current asset focused model to a systems approach, the changes being proposed within the body of revised and retired definitions appears to go well beyond what we understand was intended within the currently approved SAR. In addition, the revisions will create a significant change to existing processes, and documentation, due to revising the foundation of the identification of CIP Assets.

With the removal of the term, Cyber Asset, the SDT will be removing the necessary tie to BCS, and in turn, revising the current filtering system that Entities use to identify their CIP Assets. Additionally, with the removal of BCA, there is no explicit language within CIP Glossary Terms that address non-programmable devices as non-CIP applicable assets.

NV Energy believes that the SDT should retain the defined terms “BES Cyber Assets (BCA)” and BES Cyber System (BCS) as currently written. We also believe that given the proposed revisions made to the term “Cyber Asset,” which clarify that physical or virtual hardware, software and data are allowed, obviates the need to revise the other definitions.

NV Energy also believes that the revisions to the definition provide no improvement to reliability and security, and mainly address possible confusions found during auditing of the standards.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Please clarify “regardless of redundancy” with respect to the “combination of hardware, software, and date.” Redundancy in this context appears to relate more to the BCA definition. With respect to redundancy, as stated in CIP-002-5.1a, relative to Real-Time Operations, “…redundancy does not mitigate cyber security vulnerabilities.” Revisions to the BCS definition may cause entities the burden of redefining and modifying their classification process, as well as subsequent processes/workflows that are intertwined. Not all BCS include virtualization. The retirement of the use of the term BCA affects how audit evidence in currently proposed in “CIP Version 5 Evidence Request v2.0”. In v1.0, there were tabs for both virtual systems and BCS, in v2.0, both are eliminated. How will device sampling be handled?

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

By removing the term “programmable” and the tie to “BES Cyber Asset” (which removes the tie to “Cyber Asset”), the term BES Cyber System does not provide a clear means to exclude devices that are hardware with built-in programmable read-only memory (PROM) or can only be interacted with through a push-button interface (or similar physical interaction). Including these devices in CIP cyber security scope creates administrative burden with no clear benefit to cyber risk. Previously, these could be excluded by an entity using internal definition/clarification of “programmable” to indicate programmable through an electronic interface and without disassembly of the device (i.e. replacing a PROM chip).

Suggested options:

Cyber Asset: A programmable electronic device, including the hardware (physical or virtual), software (including application virtualization), and data in these devices.

BES Cyber System: Any combination of Cyber Assets, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused, would result in adverse impact to one or more BES Facilities within 15 minutes.

Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Please see Texas RE's response to #3.	
Likes 0	
Dislikes 0	

Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Comments: PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. Not using Cyber Asset in the definition of BES Cyber Systems removes the necessary ties between the two terms. The terms should be used as a filtering mechanism to scope the assets subject to the CIP standards. Starting with Cyber Asset being the largest population of devices, followed by a filtering process to determine whether the Cyber Assets are part of a BES Cyber System. PAC suggests adding either Cyber Asset or programmable into the proposed BCS definition. **Option 1: BES Cyber System** - Any combination of [Cyber Assets, that includes] hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes. **Option 2: BES Cyber System** - Any combination of [programmable electronic devices, that includes] hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.	
Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

The new definition expands the scope of devices that would fall into CIP regulation if the Cyber Asset term is removed by removing the BCA component. Currently only programmable electronic devices are in scope. The new definition would bring into scope electronic devices that are not capable of being updated; no means to update the software or firmware within them (not field updateable). These devices currently do not meet the "programmable" electronic device definition and are thus out of scope for NERC CIP.

The NSRF recommends leaving the BES Cyber Asset and, BES Cyber Systems definitions and accepting the proposed Cyber Asset definition. We feel this allows for virtualization and significantly reduces the documentation changes that would be required by the elimination of the BCA definition.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

We disagree with the proposed BCS definition. The NERC CIP requirements are generally device-centric, which are working well for both physical and virtual CIP Cyber Assets in registered entities' CIP compliance programs. In our virtual environment, we have no issue for continuously using the device-centric approach for the CIP compliance. For instance, we have identified the VM and SAN as a distinct virtual programmable device. CIP Version 5 previously introduced the concept of BES Cyber Systems to assist registered entities performing and documenting compliance actions by reducing the amount of required compliance documentation, and in some cases, to allow one BES Cyber Asset in a BES Cyber System to perform required actions on behalf of other BES Cyber Assets in the BES Cyber System. These BCA and BCS terms used in the registered entities' CIP compliance process today work fairly smoothly. In addition, the new term BES that breaks down from the Cyber Asset level to the hardware and software level is not manageable and auditable, and it would create additional identification workload that has no value for the registered entities. Based on the above rationale, there is no need for redefining the BCS from a compliance and security perspective. We disagree with the PCS definition for the same reason.

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
Due to the proposed retirement of the BCA definition and because the designation of the new Cyber Asset term is intentionally limited to TCA, Removable Media, and CIP-010 we believe the proposed BES Cyber System definition needs further clarification. As an example, the term “programmable” in the BCA definition currently excludes certain BCS Elements, such as Current Transformers [CT] and Potential Transformers [PT] for transmission protection BCS. Since these devices, if rendered unavailable, degraded, or misused, could cause failure of the host transmission protection BCS, the new definition of BCS could be interpreted to include all such nonprogrammable elements within a given BCS as part of the specific combination of hardware, software, and data.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Entities need guidance on what makes up a BCS. The term programmable gave sufficient guidance that cyber assets were of concern.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	

Comment
Reclamation does not support retiring the term BES Cyber Asset. Reclamation recommends the term BES Cyber Asset be retained and used as it is currently defined in all applicable definitions in the NERC Glossary of Terms. Reclamation also does not support the proposed definition of BES Cyber System. Defining BES Cyber System without using the term “BES Cyber Asset” (to include the term “programmable”) could bring equipment like PTs, CTs, pressure sensors, temperature sensors, and other hardware devices for BES functionality into scope. If the above recommendation is not adopted, Reclamation proposes the following definition of BES Cyber System: BES Cyber System – One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one o r more Facilities, systems, or equipment, which 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.

Likes 0	
Dislikes 0	

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	

Comment
Eliminating the word “programmable” blurs the line between a cyber asset and complex electrical or electronic hardware, such as non-programmable relays. It opens the door to enforcement on many more assets that don’t make sense, such as integrated appliances or complex semiconductor switching devices that do not have field-changeable firmware. The important nuance provided by the word “programmable” is that it is possible for the executable code to be modified in the field, other than just changing settings in a faceplate menu. That makes the CIP Standards relevant as protections against the device being a target for attackers (BCS) or being reconfigured for use in an intrusion or attack (EACMS, PACS, PCA). There may be value in adding a defined term for “Programmable.” A possible definition could be “containing executable code, including binaries and scripts, that can be modified after manufacture or creation. This is an intrinsic characteristic, not a situational one, which does not change with respect to whether the end user connects, secures, removes, or blocks any access paths that can used to modify executable code. This does not include the ability to modify basic configuration data that are not executed sequentially as scripts, such as a setpoint or IP address.”

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

We do not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). While we understand the SDT's desire to move from the current asset focused model to a systems approach, the changes being proposed within the body of revised and retired definitions appears to go well beyond what we understand was intended within the currently approved SAR.

We believe that the SDT should retain the defined terms "BES Cyber Assets (BCA)" and BES Cyber System (BCS) as currently written. We also believe that given the proposed revisions made to the term "Cyber Asset," which clarify that physical or virtual hardware, software and data are allowed, obviates the need to revise the other definitions.

We recommend returning the "programmable" language to the BCS definition, as well as maintaining a definition of BES Cyber Asset as a component of the BCS. We believe these changes improve backward compatibility.

This proposed change ripples into CIP-002 because Entities will need to re-evaluate their CIP-002 what is IN vs OUT. For example, some ROM devices may fall under CIP-002. This subtle change may force a new version of CIP-002 assessment - the new definition would bring in more devices that would not be considered programmable and the changes would not be backward compatible.

New definition will bring in more devices (ROM, firmware, etc.) that are typically not considered programmable

Since the Standard should be technically agnostic, we recommend not calling out virtual hardware (virtualization).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

MEC does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the "how to comply" with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

MEC believes that the SDT should retain the defined terms “BES Cyber Assets (BCA)” and BES Cyber System (BCS) as currently written. We also believe that given the proposed revisions made to the term “Cyber Asset”, which clarify that physical or virtual hardware, software and data are allowed, obviates the need to revise the other definitions.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Dominion Energy has comments on the following proposed definitions:

- PAMS – It is unclear if the intent is to collect visitor logs (paper or substation voice system).
- LIZ – 1) It is unclear if an entity has multiple VLANs behind the firewall that the entity could claim it’s in a single ESP under the proposed definition. In addition, it is unclear if an entity can mix logical isolation zones in virtual environments on a single piece of hardware. Additional clarity should be added around which entity actually defines the LIZ (either the ERO or the Entity). Finally, it is unclear on whether the communication links mentioned in 4.2.3.3apply only if the ERO determines it extends one or more geographic locations.
- IRA – Additional clarity needs to be added on what “remote access client” means. It could be interperted to be either protocol or client.
- RM – Please clarify the first bullet. Would this apply to flash drives that are smart/have chips in them? We recommend adding the examples back for clarity.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS does not agree with the proposed change in the BCS definition, unless the new Cyber Asset term is added to the definition of BCS to maintain the reference to/inclusion of the term “programmable.” Specifically, the revisions to BCS do not adequately describe the Cyber Assets that would comprise a BCS without the use of the word “programmable” because the fact that a Cyber Asset is “programmable” sets the foundational criteria by which assets and/or BCS are considered for CIP categorization. Without a reference to the term “programmable,” an inconsistency between the term Cyber Assets and BCS is introduced as is the potential that the scope of assets to be considered under the BCS classification will be unclear. To

ensure consistency and reduce the potential for confusion, AZPS requests that the term “programmable” be included in the new BCS – either directly or indirectly through replacement of “hardware (including virtual hardware), software (including application virtualization), and data” with “Cyber Assets”.

Further, AZPS notes that the Standards Authorization Request form for this Project (“the SAR”) outlined that the SDT would be responding to the V5TAG Transfer Document request for clarification of “the intent of ‘programmable’ in Cyber Asset, and a focus on the definition of ‘BES Cyber Asset’ so that it does not subsume all other cyber asset types.” AZPS notes that this draft does not provide the necessary clarity regarding the intent of “programmable” and may go beyond the scope of the SAR by retiring the term BES Cyber Asset and fundamentally changing definitions and the requirements in which they are utilized across all CIP Standards.

For these reasons, AZPS requests the rationale for how the retirement of the term BES Cyber Asset and the modifications to BCS meet the intent of the SAR as well as clarification on the reasoning (generally) behind the retirement of the term BES Cyber Asset and the removal of references to “programmable” that results from the proposed revisions to the two foundational definitions associated with the CIP reliability standards (BES Cyber Asset and BCS). As discussed above, AZPS suggests additional revisions to recapture the term “programmable.” An alternative approach could be to develop a new definition and/or classification for virtualized assets, which definition/classification would then be added to the applicability tables, as appropriate.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

The new definition expands the scope of devices that would fall into CIP regulation if the Cyber Asset term is removed by removing the BCA component. Currently only programmable electronic devices are in scope. The new definition would bring into scope electronic devices that are not capable of being updated; no means to update the software or firmware within them (not field updateable). These devices currently do not meet the “programmable” electronic device definition and are thus out of scope for NERC CIP.

We recommend leaving the BES Cyber Asset and, BES Cyber Systems definitions and accepting the proposed Cyber Asset definition. We feel this allows for virtualization and significantly reduces the documentation changes that would be required by the elimination of the BCA definition

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No

Document Name	
Comment	
The new BCS definition exludes the use of the term “Cyber Asset”. “Cyber Asset” was also redefined and used in other defined terms such as TCA’s, etc. To be consistent, we suggest the following definition for BCS “A single or combination of Cyber Assets, regardless of redundancy, performing one or more….” Since the new definition of Cyber Asset is inclusive of the hardware (physical or virtual), software and data in the devices, it makes sense to utilize the term consistently in other new/revised definitions since not all devices lend themselves to be “systems”. (i.e. stand-alone assets or components of a system).	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
By excluding the term programmable from the proposed BCS definition, the SDT risks bringing into scope devices that were previously excluded from BCSs due to not being programmable. In the guidelines and technical basis of CIP-007-6, an unmanaged switch is listed as an example of a nonprogrammable device. As a nonprogrammable device, an unmanaged switch did not meet the definition of a Cyber Asset and therefore could not meet the definition of a BES Cyber Asset. Under the proposed BCS definition, an unmanaged switch meets the BCS definition. An unmanaged switch is hardware, it contains software (the firmware the switch is running), and it contains data (the MAC address table). If this proposed change is implemented in its current form then entities may need to re-evaluate the criteria used to determine what devices should be included in BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP does not agree that the BCS definition describes the BCS appropriately. The new definition is attempting to combine many definitions into one. SRP suggests using the language below:	

A BES Cyber System includes any combination of programmable hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, where:

1. It/they performs one or more reliability tasks; and

2. If rendered unavailable, degraded, or misused, the situation would result in adverse impact to one or more BES Facilities within 15 minutes.

Additionally, the term ”programmable” should remain in the definition of a BES Cyber System. “Programmable” excludes certain IT network components such as patch panels, patch cables, etc. which should not be in scope.

SRP also agrees with APPA’s comments.

Likes 0	
Dislikes 0	

Response

Jamie Prater - Entergy - 5,6

Answer	No
Document Name	

Comment

The removal of the BCA term and failure to include programmable in BCS can potentially expand the scope of applicable devices to an entity.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Support MRO NSRF Comments

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests further clarification on the proposal for BCS definition. The proposed definition indicates that there should be a “combination of hardware, software, and data”. Is it the drafting team’s intent there must be a combination of any of those elements (hardware, software, data), or can something be considered as a BCS if it contains only one of those elements (software)? Without the use of the term “programmable” can an entity infer that an asset that is hardware only, not be considered a BCS?	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
WAPA does not support retiring the term BES Cyber Asset. WAPA recommends the term BES Cyber Asset be retained and used as it is currently defined in all applicable definitions in the NERC Glossary of Terms. WAPA also does not support the proposed definition of BES Cyber System. Defining BES Cyber System without using the term “BES Cyber Asset” (to include the term “programmable”) could bring equipment like PTs, CTs, pressure sensors, temperature sensors, and other hardware devices for BES functionality into scope.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is concerned that ultimately, this will depend on the audit methodology. If the objective of the requirement is measured to see if it is met on the BCS as a whole, then this should work. If the objective is measured on every physical device in the system, then it will fail. The term "Programmable" may still be needed as a scoping mechanism if the audit approach does not change to match the system approach.	

Southern Company is also concerned that in using the phrase “adverse impact to one or more BES Facilities”, auditors may interpret this as a considerable expansion of the scope of what is encompassed by the definition.

We understand that the F in Facility has been capitalized by the SDT intentionally and in this definition, means:

“A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)”

Therefore, it appears to Southern that this is **not** intended by the SDT to expand the scope of what is currently included, out to systems such as Fire Protection Systems, HVAC and other systems which do not have a direct impact upon the BES. Southern Company also believes that the way in which it is written will not change the scope of the Standard in respects to the inclusion of Control Centers and their associated Data Centers. As noted in CIP-002-5.1a,

“Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.”

As long as the intent behind the quote above from CIP-002 does not change in future revisions, Southern feels the intent remains the same with the proposed wording of the definition of Cyber Asset as it relates to “BES Facilities”.

Southern Company is concerned that unless the SDT finds a way to ensure that the current scope remains unchanged, our Operations groups will suffer an undue compliance burden, spending an inordinate amount of time providing evidence of minutiae while likely seeing little of the direct benefits of virtualization.

That said, Southern Company would like to see additional clarity provided in future revisions of this proposed change regarding maintaining the scope of the Standards to what is *currently* in scope. This will allow us to balance implementing the benefits of virtualization while also providing reasonable proof demonstrating a secure implementation.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer	No
Document Name	

Comment

Because the concept of “programmable” is retained in the defined term “Cyber Asset” (which is an element of a BES Cyber System), industry needs guidance on what constitutes a “programmable” electronic device. Additionally, the new definition for BES Cyber System includes electronic devices that are not capable of being updated (i.e, no means to update the software or firmware within them (not field updateable)). Therefore, because these devices currently do not meet the “programmable” electronic device definition, such devices should be out of scope for NERC CIP.

Finally, for consistency with the revised definition of Cyber Asset, the definition of BES Cyber System should read: “Any combination of physical or virtual hardware (including virtual hardware), software…”

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 no Dominion and NYPA

Answer	No
Document Name	

Comment

We recommend returning the “programmable” language to the BCS definition, as well as maintaining a definition of BES Cyber Asset as a component of the BCS. We believe these changes improve backward compatibility.

This proposed change ripples into CIP-002 because Entities will need to re-evaluate their CIP-002 what is IN vs OUT. For example, some ROM devices may fall under CIP-002. This subtle change may force a new version of CIP-002 assessment - the new definition would bring in more devices that would not be considered programmable and the changes would not be backward compatible.

New definition will bring in more devices (ROM, firmware, etc.) that are typically not considered programmable

Since the Standard should be technically agnostic, we recommend not calling out virtual hardware (virtualization).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The current definition of a BES Cyber System only includes programmable electronic devices. The proposed definition would draw in non-programmable devices. Currently non-programmable device are not in scope for CIP Compliance and should not be included since there are no means to update non-programmable devices. We recommend keeping the current definitions for BES Cyber Asset and BES Cyber System.

Likes 0	
Dislikes 0	

Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Tri-State would like clarification on how the new definition of BES Cyber Systems (BCS) will be used to evaluate Low Impact BCS. Previously the BES Cyber Asset definition could be utilized to eliminate programmable devices from being included within the Low Impact BCS. How would the new definition allow for the removal of programmable devices that while connected to a BCS, could not effect it within 15 minutes?	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BHC is concerned that the BCS proposed definition does not highlight "cyber" assets, therefore a transformer or electro-mechanical relays could be considerd part of a BCS. Additionally, the term "and data" should be removed from the BCS Cyber System definition as it is too ambiguous. BHC proposes the following definition: One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST. In addition, we ask the SDT to consider a review of CIP-002 along with the definitions of Cyber Asset, BES Cyber Asset, and BES Cyber System. The SDT’s approach to address applicability of cyber security controls to the virtualized	

functions will result in significant amount of work to make the existing documents (plans, processes and work instructions) conform to the new definitions and the risk based approach.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI members who participated in the development of these comments do not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). However, we understand that other members are more supportive of the changes. As a result, these comments do not represent a consensus, but we offer them for the SDT to consider.

EEI understands the SDT's desire to move from the current asset focused model to a systems approach, but the changes being proposed within the body of revised and retired definitions appears to go well beyond the EEI members' understanding of the scope and intention of the currently approved SAR.

EEI recommends that the SDT retain the defined terms "BES Cyber Assets (BCA)" and BES Cyber System (BCS) as currently written. Further, EEI observes that the proposed revisions made to the term "Cyber Asset," which clarify that physical or virtual hardware, software and data are allowed, obviate the need to retain the other definitions.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The proposed definition of BCS does not address the issues and interpretations that surfaced by not having a definition of "programmable."	
Likes 0	
Dislikes 0	
Response	

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
NRG asserts that the proposed definition of BCS would include the SCADA traffic itself (not just the data that exists within the hardware). Therefore, change control would need to include source control. This could be a challenge for the industry. NRG recommends that NERC SDT work to include definition delineation and classification delineation of data at rest versus data while in transit as critical relating to the definition of Cyber Asset and BES Cyber System. Expanding the definition beyond data on devices, could cause entities to have to re-define BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
The proposed definition does not address the issues and interpretations that have been raised by not having a definition of programmable. Furthermore, the definition uses the phrase “Any combination of hardware (including virtual hardware), software (including application virtualization), and data.” The term “combination” does not mean a combination including at least one of each. Instead, a combination could have a null element in a set. For instance, you could have a combination of only hardware, no software, and no data as a valid combination set. So, if you look at the definition with that in mind you could have hardware “performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.” This could easily be a breaker or some other item in a station that is made of only hardware. This has now opened a Pandora’s box of compliance issues and need for clarification rather than help resolve anything.	

We would propose that the definition say something like, “Any combination of Cyber Assets, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.” We would also prefer the term “programmable” in the definition of Cyber Asset be further clarified.	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Programmability is a fundamental concept that sets the scope of applicability for the current CIP standards. While many standards will not apply, there are a number of requirements that aren’t obviously tied to the ability of a device to be programmed. Including non-programmable hardware fundamentally changes the landscape of the CIP standards (i.e. breakers and motor-operated switches could now be in scope). Simply inserting “programmable” in front of the first instance of “hardware” in the definition would at least give the same scope as we have today (although the term “programmable” would still be fundamentally undefined and subject to individual interpretation).	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Cowlitz agrees with comments submitted by APPA. We agree with the intent of the SDT, but are concerned with the lack of clear identification/scoping towards computer systems.	
Likes 0	
Dislikes 0	
Response	

2. The SDT asserts that the proposed Cyber Asset definition provides clarity around virtual hardware. (Cyber Assets revised definition: Programmable electronic devices, including the physical or virtual hardware, software, and data in those devices.) Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See proposed Cyber Asset definition above. We believe the proposed definition is more appropriate and achieves the intended objective.	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy does not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual); however, we do not believe the change was necessary because virtualization is currently allowed under the current CIP Standards.	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon does not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual); however, we do not believe the change is necessary because the use of virtualization is not prohibited under the current CIP Standards.	
Likes 0	
Dislikes 0	

Response
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF
Answer	Yes
Document Name	
Comment
ITC is in agreement with the comments submitted by EEI: "EEI does not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual); however, we do not believe the change was necessary because virtualization is currently allowed under the current CIP Standards."
Likes 0	
Dislikes 0	
Response
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy
Answer	Yes
Document Name	
Comment
Duke Energy requests further clarification on the use of the phrase “virtual hardware”. For example, if an entity sets up a virtual switch in the “virtual hardware”, would this be considered a separate asset? Futher examples of what the drafting team considers “virtual hardware” would be beneficial to the industry.
Likes 0	
Dislikes 0	
Response
Russell Martin II - Salt River Project - 1,3,5,6 - WECC
Answer	Yes
Document Name	
Comment
SRP agrees with the definition. However SRP requests further clarification and guidance on this term as this definition will increase the scope of applicable Cyber Assets.
Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
See response to Question 1 above.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Agree. Assume the intent of the proposed definition is to include all instances of a device, even when multiple instances exist simultaneously. Virtual hardware = a logical instance of a device of which multiple versions could exist simultaneously	

Physical hardware = the physical instance of a device of which only one version can exist at a time	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
The word hardware is confusing since a hardware can't be really "virtual". We propose to use the word "virtual ware" or "virtual machine".	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	
MEC does not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual). However, we do not believe the change was necessary since we believe virtualization was not forbidden within the current body of CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Note, the proposed Cyber Asset definition included in the question is not the same as that included in Table 1 of *2016-02_CIP_Definitions_Redline_11022018.pdf*, 'A programmable electronic device, including the physical or virtual hardware, software, and data in the device.' These two definitions should be aligned.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

Cowlitz agrees with the SDT. However, consideration of the comments provided by APPA is cause for concern. The new language should not require revision of compliance efforts for non-virtual application. Cowlitz believes dual treatment as suggested by APPA is one possible solution, but placed in the definition of BES Cyber System.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

EEI members who participated in the development of these comments do not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual); however, they do not believe the change was necessary because virtualization is already permissible under the current CIP Standards.	
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 agrees with this change.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	

The Cyber Asset definition included in the question should mirror that which was included in Table 1 of 2016-02_CIP_Definitions_Redline_11022018.pdf, 'A programmable electronic device, including the physical or virtual hardware, software, and data in the device.'	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
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	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
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	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
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	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
Public power is concerned that the new definition will require new evidence and will not work with the existing approach structured around the CIP Evidence Request Spreadsheet (v2.0). Public power is also concerned that the list of BES Cyber Assets used for sampling will no longer be feasible, therefore it is not clear what approach auditors may require. In addition, documentation of the virtual host and virtual guests will only be a snapshot in time making it difficult to demonstrate compliance for individual cyber asset level security controls. APPA believes it would be clearer to maintain the BCA definition for physical devices, while providing new definitions for virtual devices (Virtual Cyber Asset), or consider a dual-definition approach (see response to Question 3).	
Likes 0	
Dislikes 0	

Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Adding “virtual” to the definition does not affect the clarity of the definition, it only includes a new subsect of devices. It may be more prudent to create a separate term and definition for Virtual Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO recommends that the SDT define “programmable” or provide guidelines regarding the difference between a non-programmable electronic device and a programmable electronic device.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
The proposed definition of cyber asset just adds the words “or virtual” to the definition, but continues to leave known issues with the current definition unaddressed. Most of these issues are related to the use of the term programmable. It is recommended that the team further evaluate the definition and consider migrating from the term programmable to a less ambiguous term. While “programmable” or a suitable variation of the term is needed, the issues with the current non-definition of programmable need to be addressed. The definition is based on programmable, the various types of programmability needs to be addressed: (1) Remotely programmable; (2)	

requires physical access and interruption of operation to change device programming; Electromechanical devices (including devices such as electromechanicable breakers and physical hardware such as communications cabling and electrical wiring)	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 2.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Please clarify the following; (1) programmable needs to be defined to provide clarity between devices that are truly programmable via logic and those that require component changes to update, (2) the meaning of application virtualization, specifically in regards to containerization, and (3) how entities are expected to inventory discreet devices to show relationship to the BCS.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC agrees with the wording recommended by AZPS. “A programmable electronic device, including hardware, software, and data in those devices, ***whether physical or virtual***.”

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	AZPS Comments - Question 2.docx

Comment

Please see the attached document.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	
Since the Standard should be technically agnostic, we recommend not calling out virtual hardware (virtualization) and do not call out physical. IOW, keep the existing Cyber Asset definition.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	
Comment	
The definition only helps address virtualization to the level of discrete virtual machines. It does not adequately cover more advanced edge cases that blur the lines between virtual machines. Examples of edge cases could include collections of machines like supercomputing clusters that share	

resources such as memory, or (more commonly) network storage. Examples could also use containerized assets, which may share a substantial amount of the OS and software without duplication, running specific software within walled containers.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

The virtual hardware is vague and causes confusion. We suggest using the previous revised Cyber Asset definition as follows:

"A programmable electronic physical or virtual device, including the hardware, software, and data in the device. Each virtual machine and host is a distinct device." Given that the virtual device can be captured separately using this previously proposed definition, additional requirements that may be developed only apply to the virtual devices if the current requirements don't fit them.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Response should be "YES". The program doesn't allow editing of the button.

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

This definition works to capture virtual hardware.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
While the revision provides some clarity around virtual hardware, “programmable” remains a debated topic that should have more clarity regarding what is programmable and what isn’t because component changes are required. The definition does not address application virtualization which is another virtualization technology that can be employed. In relation to the BCS comment, Cyber Asset needs to remain a component of BCS because otherwise how does an entity define what the composition of the System is?	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Please clarify the following: (1) programmable needs to be defined to provide clarity between devices that are truly programmable via logic and those that require component changes to update; (2) the meaning of application virtualization, specifically in regards to containerization; and (3) how entities are expected to inventory discreet devices to show relationship to the BCS.	
Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST. In addition, we recommend that the SDT focus on functionality in defining Cyber Assets (e.g. information technology and electronic components that systematically receive inputs and produce desired outputs) rather than whether it is virtual vs. physical or programmable vs. non-programable.	

Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
We believe it would be clear to keep the current BES Cyber Asset definition for physical devices and provide new stand alone definitions for virtual devices.	
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 no Dominion and NYPA	
Answer	No
Document Name	
Comment	
Since the Standard should be technically agnostic, we recommend not calling out virtual hardware (virtualization) and do not call out physical. IOW, keep the existing Cyber Asset definition.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	No
Document Name	
Comment	
What is “virtual hardware”? The SSRG recommends the SDT define virtual hardware to ensure consistent application across industry and in audit situations. Likewise, due to the programmable aspect of a Cyber Asset, “virtual” software is delivered by a vendor (rather than coded by the responsible entity) and, therefore, is not a physical programmable device (ie., hardware). Given this, how does programmable apply to virtualization software?	

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

Comments: MRO supports the intent to accommodate virtualization within the NERC Glossary terminology, but the term "device" is generally understood to be a hardware specific physical term and cannot be grammatically supported to also represent something that is virtual as has been attempted in the proposed redefinition of Cyber Asset. This grammatical conflict may yield to extensive interpretation which may hamper consistent CMEP implementation by the ERO. One option for incorporating virtual components into the Cyber Asset term could be to add a layer beneath the Cyber Asset term so that the programmable electronic devices language can remain (representing physical hardware devices), and a new defined peer term like "Virtual Programmable Asset (VPA)" or "Cyber Element" could be added to identify VPAs that have no physical form. We recommend consideration of the following terms (organized like a schema - includes hierarchy), which permit the incorporation of VPAs while insulating impact to existing NERC CIP glossary terms:

- PED (programmable electronic device) – this can remain undefined, but we understand it to be hardware based. A device is a physical thing and can't be virtual itself but can host other Virtual Programmable Assets
- Virtual Programmable Asset (VPA – more basic than a Cyber Asset): Includes software and data, but does not include physical hardware
    - Cyber Asset: PEDs and VPAs, including hardware, software, and associated data
        - BES Cyber Asset – (remains as defined)
        - BES Cyber System – (remains as defined)
        - PCA (Protected Cyber Asset) – (remains as defined)
        - EACMS – (remains as defined)
        - PACS – (remains as defined)
-
    -
        -

Likes 0	
Dislikes 0	

Response

3. The SDT asserts that the term Cyber Asset should continue to be used within the NERC Glossary of Terms for: Removable Media and Transient Cyber Asset. Due to the nature of that type of hardware, these devices do not lend themselves to the systems approach. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
SMEC agrees that the term Cyber Asset should remain in the Glossary of Terms, but does not believe it should be limited to Removeable Media and Transient Cyber Asset.	
Likes 0	
Dislikes 0	
Response	

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

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "EEI agrees that the term Cyber Asset should remain in the Glossary of Terms but does not believe it should be limited to Removeable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards utilized in its current form."	
Likes 0	

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon agrees that the term Cyber Asset should remain in the Glossary of Terms but does not believe it should be limited to Removeable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards utilized in its current form or as proposed to be revised.	
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	
CHPD agrees that the term Cyber Asset should continue to be used within the NERC Glossary of Terms for: Removable Media and Transient Cyber Asset. Additionally, consider how this same issue applies to traditional non-virtual hardware-based BES Cyber Assets. If an exception is being granted for specific existing hardware device types, then perhaps the problem should be flipped to instead consider the virtual systems to be the exception to the rule. Using this thinking, it may make more sense to instead develop separate virtualization language that is then referenced in the existing Cyber Asset and BES Cyber System definition. This would enable the language to expand scope to allow virtual environments without throwing out the existing scoping language for existing non-virtual Cyber Assets. This could be accomplished with something like the following: Virtual Cyber Asset (VCA) – Programmable virtual system that is comprised of a virtual operating system and the host hardware and software that hosts the virtual operating system. BES Cyber System (BCS) - A combination of one or more Cyber Assets or Virtual Cyber Assets performing one or more reliability tasks, including redundant members that support a reliability task, that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy agrees that the term Cyber Asset should remain in the Glossary of Terms, but does not believe it should be limited to Removeable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards utilized in its current form.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The NSRF agrees that the term Cyber Asset should continue to be used within the NERC Glossary Terms for: Removable Media and Transient Cyber Asset. The NSRF does not agree with making other changes to the Removable Media and Transient Cyber Asset definitions. Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	

We still support the current device-centric requirements for both physical and virtual devices as we are doing today rather than only for the TCA/RM. The device-centric approaches are more manageable and auditable.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Reclamation agrees that Removable Media and Transient Cyber Assets are not BES Cyber Systems. Reclamation recommends the continued use of the term Cyber Asset, not just for Removable Media and Transient Cyber Asset, but for all applicable definitions in the NERC Glossary of Terms.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	Yes
Document Name	

Comment

We agree that the term Cyber Asset should remain in the Glossary of Terms but do not believe it should be limited to Removeable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards utilized in its current form.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

MEC agrees that the term Cyber Asset should remain in the Glossary of Terms but do not believe it should be limited to Removeable Media and Transient Cyber Asset. Rather, we believe that the term should continue throughout the CIP standards utilized in its current form. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

Agree

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

Although AZPS agrees that Removable Media and Transient Cyber Assets should remain at the Cyber Asset level, this is only consistent if the changes to the definitions and/or associated approach to classification/applicability recommended in our response to Question No. 1 are incorporated.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
: See response to Question 1 above.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Support MRO NSRF Comments	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	Yes
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
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 believes the retirement of the term BES Cyber Asset accomplishes the purpose and the generic Cyber Asset is still appropriate for those areas in the standard where a device level is appropriate, such as TCAs. Due to the nature in which they are used, Transient Cyber Assets should continue to be viewed as individual assets that can be grouped for compliance and reporting reasons. The proposed changes reflect this.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

EEI agrees that the term Cyber Asset should remain in the Glossary of Terms but our members who participated in the development of these comments do not agree that it should be limited to Removable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards in its current form with its current scope and applicability.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment

Agree that TCAs should still be kept at the Cyber Asset level.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

James Grimshaw - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment

Agree that TCAs should still be kept at the Cyber Asset level.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	Yes
Document Name	

Comment

In relation to the BCS comment, Cyber Asset needs to remain a component of BCS because otherwise how does an entity define what the composition of the System is?

Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
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	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
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 no Dominion and NYPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

No comment.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment

Texas RE suggests the term Cyber Asset should continue to be used in defining all system definitions, such as Removable Media, Transient Cyber Assets, and BES Cyber System. A system is one to many Cyber Assets, regardless of whether the Cyber Asset is physical or virtual. Removing the term Cyber Asset from the system definition loses the hierarchy that is in place.

Texas RE is concerned there will be a gap because not every cyber asset in the system will be protected under the new definition. Treating the virtual machine and its host as separate Cyber Assets may result in mixed-trust virtual environments, which exacerbates vulnerabilities as the host runs CIP and corporate virtual machines. CIP controls are only being applied to the CIP virtual machine and not its host; even though the host “if rendered unavailable, degraded, or misused” can affect the CIP and corporate virtual machines. In addition to certain assets not being protected, Texas RE is concerned these changes could lead to an increased effort for entities to provide evidence of their identification of BES Cyber Systems and for Regional Entities to audit.

If the SDT elects to eliminate the term Cyber Asset, Texas RE recommends the following BES Cyber System (BCS) definition:

One or more Cyber Assets, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	

Comment

APPA believes the SDT should consider the concept of two (parallel) definitions, at least for a time, and a sort of “virtualization overlay” for the CIP Standards. Instead of replacing the definitions and Standards, create options whereby an entity can select, for any particular cyber system, to use the existing V5-6 definitions and Standards, or new virtualization definitions and Standards. It is up to the entity to make clear in advance which approach they choose for each cyber system.

As a practical matter, it is anticipated that there would be a single Standard in each case, but that it would include all the existing Parts as well as all the new proposed Parts (as modified by comments) to accommodate virtualization, with language directing an entity to select, for each cyber system, which of the two sets they will adhere to.

In this way the extensive changes to allow virtualization can be piloted by those entities most involved, while other entities can continue their CIP practices as at present, which accommodates the backwards compatibility concept. Over time, industry can learn whether the changes represent a real advance or introduce a large number of unintended consequences, and work to improve the Standards.

As such, all existing definitions would be retained in parallel to the new ones proposed in this effort.

This concept might be considered somewhat analogous to that used for the transition from PRC-005-2 to PRC-005-6, modified for use in virtualized and non-virtualized environments.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

Cyber Assets are still discrete parts of a BCS either physical or virtual and must remain a term across the standards. Limiting the use of Cyber Asset to TCA and RM becomes problematic when looking at the way a Cyber Asset that is included in a BCS is disposed of as a part of CIP-011 R2.1 and R2.2. Either the language in CIP-011 must be changed or this question needs to be rewritten to clarify the impacts to CIP-011 as well.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 3.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
The "systems" approach is flexible and has value when used for any CIP Cyber Assets. The "system" grouping can be applied arbitrarily and applicability only relies on an entities approach. In one context, the use of "Cyber Asset" versus "Cyber System" is valuable to be able to distinguish a single "device" that is included in a Cyber System. The entity just needs to be diligent in how they define their "Cyber Assets" and "Cyber Systems" to ensure they effectively provide value. We agree that Removable Media does not lend itself well to the "systems" approach. Unlike a Transient Cyber Asset (example, a laptop) that includes a combination of hardware, software, data, etc., the typical Removable Media is only media used for transferring and/or storing code and/or data.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. No changes to proposed Removable Media. PAC is suggesting some minor adjustments to the TCA definition:	

Transient Cyber Asset - A Cyber Asset that is: 1) capable of transmitting or transferring executable code, 2) not included in a BES Cyber System, 3) not [included in] a Protected Cyber System (PCS) associated with high or medium impact BES Cyber Systems, and 4) directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: 1) BES Cyber System (BCS), 2) network within a BES Cyber System Logical Isolation Zone containing high or medium impact BES Cyber Systems, or 3) PCS associated with high or medium impact BES Cyber Systems. [delete the remaining examples text] Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

BPA believes that a more effective approach would roll up the requirements that currently depend upon that term for applicability and retire the term Cyber Asset itself.

Security controls for removable media can easily be a subset of controls applied to any transient device. Rather than a defined term "Cyber Asset" which then has "Transient" pre-pended, either TCA (including removable media) can be a defined term with requirements applied to it, or the requirement can simply apply to transient devices with no special term required.

Likes 0	
Dislikes 0	

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC

Answer	No
Document Name	

Comment

Transient Cyber Assets could be better considered as Transient Cyber Systems. There may be virtualized systems that blur the line between individual or multiple assets. It may be possible to “virtually” change a Transient Cyber System’s location from inside the Logical Isolation Zone to outside, allowing it to transit. Depending on how virtualization is implemented, it may make sense to manage multiple or blurred assets on a Transient Cyber System level. The key elements of a Transient Cyber System are that the entire system is either inside the LIZ (for 30 days or less) or outside at any one time, but never both at the same time. Operating by this definition would still make asset-level management appropriate where discrete Cyber Assets such as laptops are used.

Likes 0	
Dislikes 0	

Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Has the drafting team considered modifying the terms Removable Media and Transient Cyber Asset rather than keeping the Cyber Asset definition? This may be a better approach long term, rather than keeping a term around to clarify other existing terms.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The term Cyber Asset is also used in the revised definition of ERC. We recommend keeping the current definitions for BES Cyber Asset and BES Cyber System.	
Likes 0	
Dislikes 0	
Response	

4. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicability for the monitoring portion to allow third party monitoring systems. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

We agree that the seperation allows for the utilization of a third party. We have concerns regarding the security controls that will no longer apply to the monitoring systems. This is especially concerning when considering the aggressive timeframes for response to detected conditions.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	

Comment

We appreciate the SDT clarifying the differences between access control and access monitoring and support the new definitions. We request additional details regarding the reduced applicability of the EAMS.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	

Comment

We appreciate the SDT clarifying the differences between access control and access monitoring and support the new definitions. We request additional details regarding the reduced applicability of the EAMS.

Likes 0	

Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Please clarify how an entity would classify and asset that performs and EACS and EAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify is EAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if EAMS is to be treated similar to BCSI, which appears to be the case.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
SMEC agrees with the separation of EACS and EAMS, but there needs to be more guidance provided including how to document cases when they are implemented as the same, or with overlap.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees. This will help to prioritize the protection of Electronic Access Control Systems.	
Likes 0	

Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that developing two terms for EACS and EAMS is appropriate.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We conceptually agree with the concept of splitting EACMS into EACS and EAMS. Some guidance should show clearly that EACS can be used for backwards compatibility purposes with current EACMS devices.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
These are indeed two separate classes of System (although in some cases they can be implemented as the same, or with overlap). The split will only be meaningful as it can be used to separate which Requirements are applicable to each.	
Likes 0	
Dislikes 0	

Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
We agree to separate the EACS and EAMS from EACMS. The EAMS may be treated as a BCSI repository that is allowable to be managed by the third party as long as there is a NDA in place.	
Likes 0	
Dislikes 0	

Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA suggests adding the following clarification to this question regarding security requirements for EAMS: “Under the proposed new definition EAMS can safely exist outside of a Logical Isolation Zone, under a reduced set of applicable requirements that allow entities to use additional methods to monitor and correlate access log entries.” This may require modification to CIP-004 R4.2 to allow the entity to accept verification of electronic access authorization for third parties other than at the individual level, perhaps based upon contract statements of work (SOW) or service level agreements (SLA).”	
Likes 0	
Dislikes 0	

Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
More guidance is needed to apply these new definitions to management systems like patching management, SIEMs, Anti-Virus, vCenter. Should these systems be consider EACS or EAMS?	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Using these services, third parties will still fall under the CIP-004-7 PRA requirements and access control of BCSI in CIP-011-2.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Button respons should be "No". Editing of the button isn't possible. PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. PAC believes that this can still be accomplished by maintaining the EACMS term and altering the existing definition. It will allow entities the flexibility to define the different devices that are EACMS and what duties they perform. Third party monitoring still fits into the scope of the original definition of EACMS. Based on the current proposal of EAMS and EACS, systems like SEIM and IDS would be categorized as EAMS. EAMS does not show up in any of the current draft versions of the Standards, it is unclear if this was the SDT's intent. Proposed change to existing definition for EACMS: **EACMS** - Cyber Assets or [systems] that [delete – perform] [provide] electronic access control or electronic access monitoring of [delete - the Electronic Security Perimeter(s) or] BES Cyber Systems. This includes Intermediate Systems.	
Likes 0	
Dislikes 0	
Response	

James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
I do not foresee a big impact for CPS Energy with the split of EACMS in two.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Please clarify how an entity would classify an asset that performs EACS and EAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify whether EAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if EAMS is to be treated similar to BCSI, which appears to be the case.	
Likes 0	
Dislikes 0	
Response	

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We suggest adding the following clarification to this question regarding security requirements for EAMS: "Under the proposed new definition EAMS can safely exist outside of a Logical Isolation Zone, under a reduced set of applicable requirements that allow entities to use additional methods to monitor and correlate access log entries."	
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 believes that this change is one that will allow for more granular scoping and grouping of systems so that protections can be consistently applied at appropriate levels. Along with the proposed term PAMS, the additional flexibility that this change will provide opens up the possibility to use security and analysis services that cannot currently be used while preserving backward compatibility. Southern agrees with this direction and believes it will greatly help with the sharing of logging information for detection of cyber-attacks and indicators of compromise. It is a big step towards allowing correlation of events with non-CIP network activity and the sharing of information with entities or agencies that may have classified intel for use in the analysis of log data. Southern requests that as the SDT considers this area and its relationship to BCSI, that the SDT consider the implications to “off premise repositories” of this log information that is shared with external parties for further analysis. Southern believes the risks of this should be covered contractually with NDA's for example, and not covered by system level requirements on the off-premise systems on which this data resides. With that in mind, Southern suggests the SDT consider the need for EAMS and PAMS definitions. Also, while CIP-011-2 was not included in this round of informal comments, the scope within CIP-011-2 will need to be refined to accommodate the new terms but we understand that this further refinement is planned.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
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	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	

Cowlitz supports APPA comment.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	
Document Name	

Comment

abstain

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

With respect to the proposed EAMS definition, what is meant by “Cyber systems that provide electronic access monitoring”? Is the term intended to refer to systems that are monitoring the “electronic access”? Or does the term mean that EAMS are performing electronic monitoring of the BCS (such as Tripwire, patch management solutions, SIEM tools, etc.)?

The EACS definition is clear that a device/system is controlling electronic access to the BCS.

Guidance on EAMS should include what systems are anticipated to be considered EAMS. Currently, EAMS are only applicable under CIP-004. In the event of a third-party service monitoring EAMS and PAMS, it may be extremely difficult to authorize access and revoke access in a timely fashion for individual employees at said third-party service. This requirement will need further compliance guidance. As written now, the Standard introduces for EAMS and PAMS the same unresolved challenge as exists the use of third-party cloud providers for BCS storage.

The EACMS vs. EAC/EAM definition discussion presents the same possibility for two parallel definitions as discussed above in response to Question 3. Why not retain the EACMS definition and introduce the new option for EAC/EAM definitions as well? Entities must state which definition they use for each applicable cyber system. There is no security necessity at this time to force all to change to accommodate virtualization, when only some entities are pursuing such approaches. Both options are feasible at present.

Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE does not agree that separating EACMS into two separate terms is necessary. It appears that separating EACMS into EACS and EAMS and updating the applicability of various requirements based on this new distinction is acting to remove the applicability of some requirements, including security, from purely monitoring systems. This would decrease cyber security and the defense in depth posture. Based on the changes in the applicability to EAMS that were proposed, such as CIP-004-7 R3 regarding PRAs, it appears as though we would be allowing for third party monitoring by removing requirements that are difficult for entities to impose on third parties.

In regards to the language of the proposed ECMS and EAMS definitions, the SDT uses “cyber system”. This is not consistent with the language used in the proposed BES Cyber System definition. Entities also use virtualization for their EACMS. Texas RE proposes that the EACMS definition also use the Cyber Asset term, and the Cyber Asset term will allow for virtualization.

Rather than breaking EACMS into two terms, Texas RE recommends the following revised EACMS definition:

Cyber Assets that perform authentication, monitoring and logging, access control, interactive remote access, or alerting of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

This recommendation is based on FERC’s description of EACMs in Order 848, paragraph 54: “*With regard to identifying EACMS for reporting purposes, NERC’s reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. Those functions must include, at a minimum: (1) authentication; (2) monitoring and logging; (3) access control; (4) interactive remote access; and (5) alerting*.”

Likes 0	
Dislikes 0	

Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

The only place EAMS is used is in CIP-004 R4 relative to granting physical and electronic access. Please clarify the definition of EAMS. Do EAMS monitor “electronic access” to a BCS or Cyber Asset within a BCS, or does it refer to event monitoring and network inventory discovery tools like SIEMs

and Tripwire, Spiceworks, etc? If third party monitoring is allowed, how can the entity timely handle revocation of access? Logging and alerting in CIP-007 R4 refer to EACS however; the proposed definitions do not apply to those terms and are better suited for EAMS.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy agrees with the SDT that there are potential future benefits in separating the control and monitoring functions of EACMS; however, we do not agree these changes should be pursued at this time. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. The changes provided by this separation of functions by device, at this time, will again represent another overhaul of existing Entity's CIP programs, processes, and documentation.

Additionally, the current SAR simply asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards, along with assessing the security risks associated with virtualization. We do not believe this should be interpreted to mean that the SDT should as a first step recraft the body of CIP Standards in ways that fundamentally change the current BES Cyber System security philosophy. While that may ultimately be what is necessary, we do not believe that is what is required at this time. We are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.

For this reason, we recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization.

Additionally of note, that there are no Parts within the revisions to the Standards that are applicable to EAMS, which would question the need for splitting the EACMS definition versus revising the definition to accommodate the SDT's intent.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CenterPoint Energy) does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The intent of the new EACS and EAMS terms need to be clarified. The SDT should consider adding “access monitoring, alerting, and logging” to the EAMS definition to be consistent with the approach for PACS and PAMS. The definition should also clarify that the alert is coming from the system generating the alert.	
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	No
Document Name	
Comment	
This change will require all existing non-third party systems that perform both operations to be re-classified under two Cyber Asset definitions, rather than one. Consider retaining the existing EACMS classification and adding new split classifications that can optionally be used for those systems that only perform half of the functional activities.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 4.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	

Exelon agrees that there are potential future benefits in separating the control and monitoring functions of EACMS; however, we are concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it. More work needs to be done to identify the risk/reward scenarios and what controls would be applied on entity based EAMS vs vendor/cloud based EACS. We also question the backward compatibility of this change, as it drives documentation, compliance tool/technology and process changes.

Overall, we do not agree these changes should be pursued at this time and under this effort. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. We recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization, and 4) consider aligning to NIST or other existing security objective-based frameworks where possible.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"EEI agrees that there are potential future benefits in separating the control and monitoring functions of EACMS; however, we do not agree these changes should be pursued at this time. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. Specifically, the SAR simply asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards along with assessing the security risks associated with virtualization. We do not believe this should be interpreted to mean that the SDT should as a first step recraft the body of CIP Standards in ways that fundamentally change the current BES Cyber System security philosophy. While that may ultimately be what is necessary, we do not believe that is what is required at this time. We are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.

For this reason, we recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization."

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Although N&ST appreciates the desire to allow the use of 3rd party monitoring systems in CIP environments, N&ST strongly opposes the idea of allowing “monitoring only” devices to be assigned to a new definition and subject to only CIP-004 requirements. N&ST believes this proposal suggests the SDT considers detective security controls to be of lesser importance than preventative controls, which in our opinion is contrary to generally accepted best practices for layered and multi-faceted cyber security. N&ST notes that the SANS / E-ISAC analysis of the Ukraine power grid attack cites a lack of ICS network monitoring as a likely factor in the attack’s success. N&ST further notes that in FERC Order 850, in which the Commission directs NERC to add EACMS devices to the applicable systems for Supply Chain Standards, the Commission specifically argues against the idea that monitoring may be a less important security function (Paragraph 57).

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

In addition, if an entity is using a single system for both EACS and EAMS, how should the system be identified within CIP-002 (as a EACS, EAMS or EACS / EAMS combination), and should the system be high-water marked within applicable standards and requirements?

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
More clarification is needed regarding the phrase “Cyber System”. The drafting team is proposing a definition of “BES Cyber System”, but there is no definition for “Cyber System”. Is it the drafting team’s intent that an entity should create its own definition for “Cyber System”?	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No

Document Name	
Comment	
Support MRO NSRF Comments	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA agrees with ERCOT's comment. Please clarify how an entity would classify an asset that performs and EACS and EAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify - is EAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or is EAMS is to be treated similar to BCSI, which appears to be the case?	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
By separating EACMS into EAMS and EACS, it will allow entities to place "monitoring systems" (EAMS) outside of a PSP and be treated similarly to BCSI. While this concept makes sense from an information protection perspective, it dramatically increases risk to the safe and reliable operation of the BES. EAMSs are more than just BCSI containers - they may also perform alerting to potential/actual cyber attacks. Permitting them to reside outside of a defined PSP (refer to EAMS removal in CIP-006-7 Redline) increases the risk of their physical impairment by an attacker. Furthermore, the implementation of EAMSs in either a corporate enterprise or 3rd party environment, potentially outside of a PSP and/or DMZ associated with a LIZ, extends the surface area for a cyber attack and increases the number of potential attack vectors. As a result, it would place BCSs/PCSs at greater risk of an undetected attack. Since CIP-004-7 continues to include EAMSs in requirements associated with granting and revoking electronic access, the use of 3rd party providers to support EAMSs will become increasingly difficult to manage. 3rd party providers would also have to agree to requirements in other CIP standards such as “disposal of cyber assets containing BCSI”.	

If EAMS and EACS functionality cannot be split from a device, it's unclear as to how it should be categorized.

Recommendation: These changes are not impacted by virtualization and should be left as-is.

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

This proposed retirement could have impacts on other Standards, especially CIP-008, that need to be considered.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the "how to comply" with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	

Comment

We agree with the split but are concerned of security implications. We request more guidance. Could this approach reduce an Entity's security posture for the sake of meeting compliance? Could this split result in compliance confusion on applicability? How would an Entity correctly classify these assets? We suggest this change drives documentation changes and probably tool/technology changes, so we question this backwards compatibility

We agree that there are potential future benefits in separating the control and monitoring functions of EACMS; however, we do not agree these changes should be pursued at this time. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. Specifically, the SAR simply asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards along with assessing the security risks associated with virtualization. We do not believe this should be interpreted to mean that the SDT should as a first step recraft the body of CIP Standards in ways that fundamentally change the current BES Cyber System security philosophy. While that may ultimately be what is necessary, we do not believe that is what is required at this time. We are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.

For this reason, we recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	

Comment

Reclamation recommends NERC not retire EACMS. Reclamation does not support creating new terms EACS and EAMS. If EACMS must be retired, Reclamation recommends using existing, familiar industry terms (as defined in the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298)).

For example:

Replace **EACMS** with NIST's **Intrusion Detection and Prevention System (IDPS)** – Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Replace **EACS** with NIST's **Intrusion Prevention System(s) (IPS)** – System(s) that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Replace **EAMS** with NIST's **Intrusion Detection Systems (IDS)** – System(s) that detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
If the EAMS contains BCSI then how is third party monitoring allowed? A company still must protect BCSI. More guidance is required for how third party-managed EAMS containing BCSI can be done in a compliant manner. In addition, v5 has an assumption that BCS, PACS, and EACMS are always separate devices. However, they are not. Now we have split EACMS into two along with PACS. So, what is required of devices that have multiple associations? This needs to be address by the SDT.	
Likes 0	
Dislikes 0	
Response	

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
NRG asserts that this could have the biggest implication to CIP-004 and CIP-007. This could cause difficulty for the industry to acheive reliability and security due to a broadening of the standards to include serial ports. As an example intrusion detection systems would be required to alert on activity that was not previously configured under the standard.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI agrees that there are potential future benefits in separating the control and monitoring functions of EACMS; however, our members who participated in the development of these comments do not agree that these changes should be pursued at this time. The changes being considered by the SDT go well beyond the intended scope provided within the approved SAR. Specifically, the SAR asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards along with assessing the security risks associated with virtualization. However, the SDT appears to be recrafting the body of CIP Standards in ways that fundamentally change the current security philosophy. While that may ultimately be what is necessary, it may not be required at this time to support inclusion of virtualization within the CIP reliability standards. EEI members are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.	

For this reason, EEI recommends that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities considering the implementation of virtualization.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
If EACMS is split into EAMS and EACS, what would be considered an EAMS? The camera systems or software used to perform electronic monitoring? CIP-007 and CIP-010 only require Electronic Control Systems (EACS) and no Electronic Monitoring Systems (EAMS). So an entity has to control access but does not have to monitor it, was this the intent of the SDT?	
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 no Dominion and NYPA	
Answer	No
Document Name	
Comment	

We agree with the split but are concerned of security implications. We request more guidance. Could this approach reduce an Entity's security posture for the sake of meeting compliance? Could this split result in compliance confusion on applicability? How would an Entity correctly classify these assets? We suggest this change drives documentation changes and probably tool/technology changes, so we question this backwards compatibility	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	

5. The SDT realized through the process of splitting EACMS that the same considerations apply to PACS, which will allow changes within the applicability for alerting and logging (PAMS is not reflected within the applicability section at this time). The SDT is considering splitting the PACS term into PACS and PAMS to allow third party monitoring or event correlation to be performed without carrying the PACS classification. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
SMEC agrees with the separation of PACS and PAMS, but there needs to be more guidance provided including how to document cases when they are implemented as the same, or with overlap.	
Likes 0	
Dislikes 0	
Response	

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
LES is in favor of the changes, however we are concerned about the undefined term of "Cyber systems" found in several of the proposed new definitions. LES woudl like to see "Cyber systems" defined.	
Likes 0	
Dislikes 0	
Response	

Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Please clarify how an entity would classify and asset that performs and PACS and PAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify is PAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if PAMS is to be treated similar to BCSI, which appears to be the case.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support a similar approach for PACS as stated in question number 4 above. This will remove any disincentive for additional monitoring of systems.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
We support a similar approach for PACS as stated in question number 4 above. This will remove any disincentive for additional monitoring of systems.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

We agree that the seperation allows for the utilization of a third party. We have concerns regarding the security controls that will no longer apply to the monitoring systems. This is especially concerning when considering the aggressive timeframes for response to detected conditions.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

Button response should be "No". Editing option seems to be broken.

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

PAC believes this can still be accomplished by maintaining the PACS term and altering the proposed definition. It will allow entities the flexibility to define the different devices that are PACS and what duties they perform. Third party monitoring still fits into the scope of the original definition of PACS. Based on the current proposal of PAMS, there are no instances of the term used in the proposed Standards, it is unclear if this was the SDT's intent.

Proposed change to PACS:

PACS - Cyber Assets [or systems] 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.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	Yes
Document Name	

Comment

The same comments as the above question 4.

Likes 0	
Dislikes 0	

Response
Leonard Kula - Independent Electricity System Operator - 2
Answer	Yes
Document Name	
Comment
No comment
Likes 0	
Dislikes 0	
Response
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6
Answer	Yes
Document Name	
Comment
AZPS agrees that the same considerations that are applied to EACMS should be applied to PACS.
Likes 0	
Dislikes 0	
Response
Russell Martin II - Salt River Project - 1,3,5,6 - WECC
Answer	Yes
Document Name	
Comment
SRP agrees.
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 enthusiastically agrees with separating the monitoring/logging aspects out of the access control systems. However, we suggest the SDT consider the need for EAMS and PAMS to exist at all. The monitoring and logging aspects of these systems make any risk they present a data disclosure risk and not a device or system-oriented risk. If the data is of concern, we can have requirements to protect the data without the need for device/system level terms at all. Also, please see our answer to question 4.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
If EACMS is split in two, it makes sense for PACS to also be split.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Please clarify how an entity would classify an asset that performs PACS and PAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify whether PAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if PAMS is to be treated similar to BCSI, which appears to be the case.	
Likes 0	

Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
If EACMS is split in two, it makes sense for PACS to also be split.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
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	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	

Document Name	
Comment	
While public power is not sure of the need to separate the terms, if the terms are separated, they will require appropriate accompanying guidance. Consistent with our EAMS response in question 4, clarity regarding applicability of the terms would be needed. The SDT should consider the additional resources and costs associated with a registered entity adding the new applicability to existing CIP-004, R4, and R5 requirements. Moreover, the EAMS and PAMS would need to be incorporated into CIP-011 as designated storage locations. As indicated in the responses to questions 3 and 4, another option is to retain the existing definition while introducing the option to use the new bifurcated formulation, which may offer advantages to some. In this case, the existing PACS term might be re-named PACMS (in parallel with EACMS) so that PACS and PAMS are clear and also parallel to new terms. APPA would also request that the SDT consider the CIP controls appropriate for PAMS. As is the case for EAMS, if defined and scoped carefully, a PAMS may have no 15-minute impact and would not qualify for CIP controls at all, other than potentially as a BCS storage location	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	
abstain	
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 no Dominion and NYPA	
Answer	
Document Name	
Comment	
abstain	
Likes 0	
Dislikes 0	

Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	
Cowlitz supports APPA comment.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
If an entity is using a single system for both PACS and PAMS, how should the system be identified within CIP-002 (as a PACS, PAMS or PACS / PAMS combination), and should the system be high-water marked within applicable standards and requirements? NYPA questions why PAMS is excluded from certain requirements, such as CIP-006 R1.7 (alarm or alert for detected unauthorized physical access) or R3.1 (Maintenance and Testing). If entities rely on PAMS for alerting and logging within CIP-006 R1, these systems should be subject to M&T processes. And if the new definition of PAMS focuses on alerting and logging, this system should be applicable to R1.7. Excluding PAMS from selected requirements is lowering the security bar. In addition, the SDT should justify why PAMS and EAMS are specifically called out within the requirement language of CIP-004 R4.1, 4.4, and 5.3. This approach is inconsistent throughout the standards and exclude other applicable device types listed within the ‘Applicable Systems’ column.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST would oppose this change if it resulted in “PAMS” devices being subject to only CIP-004 requirements (as per our response to Question 4, above).

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"As stated within EEI’s response to Question 4 in consideration of the splitting of the term EACMS, we have similar concerns with the changes being proposed with PACS."

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

As stated within Exelon’s response to Question 4 in consideration of the splitting of the term EACMS, we have similar concerns with the changes being proposed with PACS.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 5.

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	No
Document Name	

Comment

Similar to EACMS, this change will require all existing non-third party systems that perform both operations to be re-classified under two Cyber Asset definitions, rather than one. Consider retaining the existing PACS definition and adding new split classifications that can optionally be used for those systems that only perform half of the functional activities.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The intent of the new PACS and PAMS terms needs to be clarified further.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy agrees with the SDT that there are potential future benefits in separating the control and monitoring functions of PACS; however, we do not agree these changes should be pursued at this time. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. The changes provided by this separation of functions by device, at this time, will again represent another overhaul of existing Entity's CIP programs, processes, and documentation.

Additionally, the current SAR simply asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards, along with assessing the security risks associated with virtualization. We do not believe this should be interpreted to mean that the SDT should as a first step recraft the body of CIP Standards in ways that fundamentally change the current BES Cyber System security philosophy. While that may ultimately be what is necessary, we do not believe that is what is required at this time. We are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.

For this reason, we recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization.

Given there is no applicability for PAMS at this time, NV Energy would recommend the SDT address the reasoning for maintaining the Glossary Term if its existence is not applicable to the CIP Standards.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

The only place PAMS is used is in CIP-004 R4 relative to granting physical and electronic access. Logging and alerting in CIP-007 R4 refer to PACS however; the proposed definitions do not apply to those terms and are better suited for PAMS.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE shares the same concerns for splitting the PACS term into the terms PACs and PAMs as it does for splitting the EACMS definition. Please see Texas RE's response to #4.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	
Comment	

Use of or considering separate systems for control or monitoring for PACS doesn't seem likely. Therefore, we do not belive the change is warranted.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

Reclamation recommends the SDT apply the same considerations used for splitting EACMS to PACS. Specifically, Reclamation recommends the SDT consider creating the term PACMS to address existing systems that both control and monitor physical access. Reclamation proposes the existing definition for PACS be used for Physical Access Control and Monitoring Systems (PACMS).

Physical Access Control and Monitoring Systems (PACMS) – 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

Reclamation supports creating the new terms PACS and PAMS if the PACMS term is also adopted.

Reclamation also recommends changing the proposed definitions of PACS and PAMS to use the term "Cyber Assets" instead of "Cyber Systems," as described in the response to Question 1,

from:

Physical Access Control Systems (PACS) – Cyber systems that control 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.

and

Physical Access Monitoring Systems (PAMS) – Cyber systems that 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.

to:

Physical Access Control Systems (PACS) – One or more Cyber Assets that control 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.

and

Physical Access Monitoring Systems (PAMS) – One or more Cyber Assets that 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, cameras, and badge readers.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	
Comment	
There is no practical way to meet Requirements related to controlling authorized access without also monitoring whether access granted by the PACS is authorized. In this way, PACS must already be integrated with a form of the proposed PAMS. It is, however, possible for monitoring systems (the proposed PAMS) to go above and beyond the minimum Requirements for PACS. Such additional functionality, which may be helpful to support additional operating controls, should be encouraged. Inventing a new asset class for PAMS would increase the regulatory burden placed on these optional but encouraged systems. The change could have the undesired effect of deterring any monitoring beyond minimum compliance, rather than the desired effect of improving system security.	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	
As stated within our response to Question 4 in consideration of the splitting of the term EACMS, we have similar concerns with the changes being proposed with PACS.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No

Document Name	

Comment

The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

Similar to our response for Question #4.

Recommendation : These changes are not impacted by virtualization and should be left as-is.

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

LCRA agrees with ERCOT's comment.

Please clarify how an entity would classify and asset that performs and PACS and PAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify - is PAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or is PAMS is to be treated similar to BCSI, which appears to be the case?	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Support MRO NSRF Comments	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	

Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
The proposed definition of PAMS contains an exclusion for locally mounted hardware or devices as the PSP such as motion sensors, electronic lock control mechanisms, and badge readers. Is it the drafting team's intent that cameras should fall under the exclusion of locally mounted hardware as well?	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
WAPA does not recommend the splitting of PACS into two separate definitions.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	

Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Industry would need clarity regarding the term PAMS. Does PACS need to be separated into two terms?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI members who participated in the development of these comments have similar concerns with the changes being proposed with PACS as are described above within EEI's response to Question 4 in consideration of the splitting of the term EACMS.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
In v5 there is an assumption that BCS, PACS, and EACMS are always separate devices. However, they are not. Now we have split PACS into two along with EACMS. So, what is required of devices that have multiple associations? This needs to be address by the SDT.	
Likes 0	
Dislikes 0	
Response	

6. The SDT is proposing to move away from the more prescriptive ESP/EAP model to logical isolation through the higher level objectives provided by the BES Cyber System concept and its Logical Isolation Zone. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	Yes
Document Name	

Comment

We agree with the concept of logical isolation but struggle with the removal of ERC from CIP-005 R2. Not all substations have ERC and therefore do not have Interactive Remote Access. What are the proposed compliance obligations and what is the best way to demonstrate?

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	Yes
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES

Answer	Yes
Document Name	

Comment

We agree with the concept, however LIZ and PCS are defined by their own terms, for example "Logication Isolation Zone: A logicial security zone...." The definitions should be worked on furhter so to avoid this circular definition. This choice of defining also makes 4.2.3.2 and 4.2.3.3 in CIP-010-4 difficult to understand.

Likes 0	

Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Although N&ST is generally supportive of this proposal, we believe there are significant issues surrounding the question of how compliance, and the use of effective controls, can be adequately demonstrated. N&ST also believes the proposed definition of “LIZ” should be modified, as per our response to Question 12, following.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
While we agree with the proposal to move in this direction, we feel that much more detailed information will be needed in the definitions to fill the void by eliminating the GTB sections. Also, we feel that this approach would benefit from an actual definition for “Logical Security Zone”. This phrase is used in the Logical Isolation Zone definition, but is not itself defined.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We conceptually agree with proposed definition for Logical Isolation Zone.	
Likes 0	

Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
This is a good move. However, more clarity is needed on the LIZ language to define what the boundaries of an LIZ are. A communication boundary may not be an accurate way to describe the boundary of an LIZ. Traditional definitions of communication do not take into account virtualized systems that share components; information, hardware, and executable code may exist in a location that bridges the communicating boundary of an LIZ. The definition of PCA may need to be expanded to include any asset, such as a hypervisor, that is able to access the internals of an LIZ. For example, if an LIZ includes virtual machines on a VMware host, the host would be a PCA. If an LIZ is containerized, the host OS would be a PCA. If the virtualized assets are on a SAN, then the SAN would be a PCA. The LIZ would need defined limits which are protected by LIZ design. CIP-005 R1.1 would remain necessary and would specify that all applicable BCS must reside within a defined LIZ. The issue would have to be addressed: How to use inclusive language that covers both routable networked devices and components of a virtualized environment, but exclude devices that are neither.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The SDT should consider clearifying the definition of BCS devices to ensure that entities can readily identify the devices and protect them with logical isolation.	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes

Document Name	
Comment	
While AEP agrees, we would like to see examples and/or diagrams of how to apply these zones at a more granular level included in Technical Rationale and or Implementation Guidance.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
This will require the logical isolation rules or policies to be reviewed holistically. Entities will need to thoroughly explain how they are logically isolating and the relation to other networks and systems that are not BCS.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Button response should be "No". Editing option seems to be broken. PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. This term captures the intent, but PAC suggests not using the same words from the term to describe the zone in its definition (i.e. logical security zone = logical isolation zone): Logical Isolation Zone – [delete - A logical] [Electronic] security zone created by applying [logical] controls to communications to or from BES Cyber Systems and Protected Cyber Systems.	
Likes 0	

Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
We agree that this helps allow entities to provide more defense in depth. However, if an Entity has multiple LIZ nested within each other and has a violation of one of the inner LIZ then you have removed the motivation to do more. If an interior LIZ has a violation but is still fully protected by an outer LIZ, then the Violation Risk Factors should reflect that only a violation related to the outer most LIZ of a nested LIZ setup should result in a penalty. However, if all the BCS and PCAs were all protected by another LIZ then the entity should not be penalized for the outermost LIZ violation since they were all within another interior LIZ. This is because the risk to the BES remain unchanged.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Less rigid term, leaves room for circumstances where ESP may have been difficult to be applied.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	

Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Less rigid term, leaves room for circumstances where ESP may have been difficult to be applied.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Hydro One supports the SDT's approach. Assuming all segmentation has to occur at Layer 3 of the OSI stack is doesn't align with current technology trends. We believe that additional implementation guidance is warranted for the industry while allowing flexibility for technical solutions.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	Yes
Document Name	
Comment	

The SSRG supports retaining the “are connected using a routable protocol” language to provide additional clarity to the definition: LIZ – “A logical security zone created by applying controls to communications to or from BES Cyber Systems and Protected Cyber Systems that are connected using a routable protocol.”

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

While the move to a higher-level view for scoping will require an additional review of our internal programs and lower level work practices, Southern Company believes that this change will allow us additional flexibility in implementing protections at an appropriate level.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
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	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	

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	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
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	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
The Technical Rationale document describes well how the Logical Isolation Zone (LIZ) concept will improve the security for virtual environments as well as clarify the serial communications. We recommend that the SDT consider adding clarification to the standard regarding DNP3 over Serial communications. Several questions remain. For example, will the SCADA communications from a front-end processor through a terminal services device to strip off IP communications for DNP3 over serial also be considered as logical isolation? Also, it is not clear why “with External Routable Connectivity” was removed from CIP-005 R2. Given that the CIP-005 Technical Rationale indicates the serial connectivity generally provides logical isolation (p.4), the “with ERC” clarifier should be retained. The LIZ concept represents another dual-definition opportunity, if ESP is retained. An entity would be able select between either concept, on a cyber-system by cyber-system basis, based on which concept makes the most sense for security and operations in its particular environment.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE does not see a need to retire the term ESP and introduce the new term, Logical Isolation Zone. The current definition of ESP provides entities the flexibility to implement ESP(s) based on network environment and technology used. ESP(s) can be established using VLANs, IP ranges, **network zones**, demilitarized zone (DMZ), etc. Changing the definition to Logical Isolation Zone means entities would need to implement "network zones", which would not allow for the same flexibility as the ESP concept. This could result in potential un-needed upgrades. Texas RE does not agree with retiring the EAP definition. Since network traffic from Logical Isolation Zones will need to pass through an interface, the definition of EAP should be retained and protected how it is currently being protected. Texas RE does agree with moving the concept of PCA to PCS, however, Texas RE recommends using the current definition of PCA and simply change the term to PCS. This is consistent with Texas RE's recommendation for the BCS definition.	
Likes 0	
Dislikes 0	
Response	

Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO supports the shift from ESP/EAP to a Logical Isolation Zone. MISO requests the SDT consider that inclusion of serial port connectivity may inadvertently expand scope to include devices such as HVAC and physical control locks.	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

NV Energy does not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ). While there may be future benefits to such a change, and NV Energy currently deploys this method of Zone identification within its system, NV Energy does not believe that this is the right time, nor do we agree that the changes being considered will improve an entity's reliability, security and compliance efforts through the higher-level objectives set forth by the SDT. Responsible Entities have broadly built their cybersecurity programs around proven concepts, objectives, and programs. The proposed changes will undoubtedly create significant disruption to those systems and efforts. We also question the need for such broad changes when there are changes within the body of CIP Reliability Standards that will not be enforceable until the year 2020 (e.g., CIP-005-6).

NV Energy is also concerned that the level of change being contemplated by the SDT is too great and represents a very steep learning curve for the industry. For this reason, we ask the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The Logical Isolation Zone (LIZ) concept does not address host firewalls or other technology limiting logical connections to an asset. The SDT should revise the LIZ definition to clarify that the LIZ controls are external to the controls applied by the BES Cyber System itself.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	

Comment

Introduction of a new term logical isolation zone rather than ESP introduces confusion in the definition and with backward compatibility. For example, the definition would now be applicable to serial communications. This is an example of a definition that will be debated for several years in the industry. Continue with our current industry standard definition or ESP and adjust the standards language to address issues or adopt standard NIST

terms. SuperESPs can be accommodated by changes to requirements rather than definitions as the current definition of an ESP does not prevent multi-site ESPs.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 6.

Additionally, Westar | Kansas City Power & Light Company share the following observations:

Retiring the Electronic Access Point Glossary Term removes critical identification of the ingress and egress points.

The concept of a Logical Isolation Zone does not relieve the expectation of documented ingress and egress points, especially for network diagramming.

Identify LIZ Data Flow. Related to concerns regarding retirement of the EAP Glossary Term, we believe it is critical that the Logical Isolation Zone considers the ingress and egress flow of data at the zone.

LIZ Residing within a PSP. Considering the Logical Isolation Zone concept, at first glance, it would be expected the LIZ is protected within a Physical Security Perimeter. The LIZ concept is strengthened by an affirmative statement the zone is located within a PSP.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

Exelon does not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ) as part of this effort.

We do agree there may be future benefits to such a change but see this being handled more appropriately within a separate, comprehensive CIP version overhaul effort. Even with the proposed backward compatibility, this change will be disruptive to current CIP programs in place, requiring documentation, compliance tool/technology and process changes. Such a change also brings with it a very steep learning curve for the industry.

We would prefer for the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational comment period.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "EEI does not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ). While there may be future benefits to such a change, EEI does not believe that this is the right time, nor do we agree that the changes being considered will improve an entity's reliability, security and compliance efforts through the higher-level objectives set forth by the SDT. Responsible Entities have broadly built their cybersecurity programs around proven concepts, objectives, and programs. The proposed changes will undoubtedly create significant disruption to those systems and efforts. We also question the need for such broad changes when there are changes within the body of CIP Reliability Standards that will not be enforceable until the year 2020 (e.g., CIP-005-6). EEI is also concerned that the level of change being contemplated by the SDT is too great and represents a very steep learning curve for the industry. For this reason, we ask the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting."	
Likes 0	
Dislikes 0	
Response	

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC believes the proposed changes to the CIP standards goes beyond the intent of the SAR. The proposed new term LIZ, if approved, should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol while keep the existing requirements the same as before. The changes as proposed will bring BES Cyber Sytems with serial conections, no erc and no dial up into scope for a number of requirements with no benefit. SMEC is concerned that this magnitude of change to the CIP standards and definitions would be too disruptive to non-virtualization compliance.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST. We stress that the SDT must better define the term “communications” used throughout the standards / requirements, and whether this expands the scope beyond routable communications. SDT should also differentiate between a logical and physical environment. The current proposed change does not provide a security benefit and will lead to costly administrative changes (governance documents, asset management systems, diagrams, evidence, etc.). NYPA supports maintaining the ESP / EAP, and routable communication model. In addition, the SDT should consider reverting to the previous CIP-005 R1.1 that required identification (boundaries) of the Electronic Security Perimeter (or Logical Isolation Zone in this case). Entities must define / develop a LIZ before applying required security controls.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	

Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Support MRO NSRF Comments	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP believes removing the term ‘routable protocol’ from the definition may bring serial connections in scope, which are currently excluded. Not excluding serial connection does not allow for backwards compatibility. Additionally, SRP agrees with APPA’s comments.	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA is concerned that the removal of language specifying the use of a routable protocol may have unanticipated consequences on compliance with requirements where devices were previously not in scope due to not being connected to a BES Cyber System through a routable protocol.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The exclusion of "Routable Protocol" in the LIZ definition, along with the technical guidance, helps address the use of serial comms and its inherent isolation ability. Note: To achieve this, on CIP-005-7 Part R 1.1, the sub Parts should be bulleted and the “and” between sub Part 1.1 and 1.2 should be an “or”. In addition, it would be preferable to put some specific language in this definition and requirements in lieu of referring to technical guidance. The redaction of EAP from the definition is detracting from the ability to easily identify what connections lead to BCSs/PCSs. Recommendation: Restate EAP definition in new terms that coincide with the implementation of a LIZ. (I.e. Entities can identify “Virtual” EAP’s by name/lable).	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No

Document Name	
Comment	

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

This will require unnecessary additional documentation for serial connected devices. We do not see an issue with the current ESP/EAP model. We support keeping the "are connected using a routable protocol" language.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

MEC does not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ). The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the "how to comply" with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	
Response	

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	
Comment	

Recommend changing the label to clarify this is a security label . . . possibly Logical Security Zones

Audit interpretations of this new, more flexible label are a concern

Concern that this does not enhance cyber security, this is not backwards compatible and forces to re-evaluate what is in scope (ie, microwave communications, serial communications, third party communications, etc). Need better clarification on communications demarcation – what is in scope vs out of scope? Concerned that the current CIP-005 R1.1 has not translated well – need more clarity on establishing boundaries and guidance on how to document

We do not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ). While there may be future benefits to such a change, we do not believe that this is the right time, nor do we agree that the changes being considered will improve an entity's reliability, security and compliance efforts through the higher-level objectives set forth by the SDT. Responsible Entities have broadly built their cybersecurity programs around proven concepts, objectives, and programs. The proposed changes will undoubtedly create significant disruption to those systems and efforts. We also question the need for such broad changes when there are changes within the body of CIP Reliability Standards that will not be enforceable until the year 2020 (e.g., CIP-005-6).

We are also concerned that the level of change being contemplated by the SDT is too great and represents a very steep learning curve for the industry. For this reason, we ask the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Reclamation does not support the proposed term Logical Isolation Zone (LIZ). "Logical isolation" in computer networking is when two sets of devices, which share a physical network infrastructure, are prevented from being able to communicate with each other. The proposed definition implies that a LIZ is a created by *controlling* the communications to and from BES Cyber Systems and Protected Cyber Systems. This is the opposite of isolation.

Logical isolation must distinguish between BES and non-BES. A Logical Isolation Zone could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on common hardware between CIP Applicable Systems and corporate business networks could also introduce risk to the BES.

Reclamation recommends retaining the existing ESP/EAP model. If the ESP/EAP model must be modified, Reclamation recommends using existing, familiar industry terms (as defined in the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298)).

For example:

Replace **ESP** with NIST's **Enclave** – A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Replace **EAP** with NISTS's **Enclave Boundary** – Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a wide area network (WAN).

Reclamation recommends the following term be added to the NERC Glossary of Terms instead of LIZ:

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

We disagree to use LIZ to replace the term ESP/EAP that is commonly understood and widely accepted by the registered entities. Given that currently the majority of CIP Cyber Assets (more than 99%) are physical devices and the ESP/EAP compliance process today works fairly smoothly by implementing ESP/EAP requirements that are appropriately prescribed, it doesn't make sense to change ESP to LIZ that is only for sufficing a very small percentage of the virtual devices while ignoring the fact that the majority of physical CIP devices are working very well for the ESP/EAP.

We suggest the proposed new term LIZ should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol while keep the existing requirements the same as before. Resulting from our suggestions, it would be beneficial for all registered entities as follows:

- For the entities that have no any virtual CIP Cyber Assets, they don't need to do anything.
- For the entities that have some virtual CIP Cyber Assets, they may need to use the new term LIZ to resolve the CIP compliance issues unless they could resolve them before.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory

Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

This will require unnecessary additional documentation for serial connected devices. The NSRF does not see an issue with the current ESP/EAP model. The NSRF supports keeping the "are connected using a routable protocol" language.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	No
Document Name	

Comment

Cowlitz supports APPA comments and the SDT's intent. The standard language must be adjusted as the current ESP/EAP model will not support virtual systems, but the concerns expressed by APPA should be considered.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

This potential standard change has a broad implication than higher level objectives provided by BES Cyber System concept (and its Logical Isolation Zone). This could cause a re-definition of Interactive Remote Access. This adds a broader compliance burden to the standards than presently required under the non ERC BCA category. The secure configuration now includes serial configuration data. NRG asserts that this potential change would broadly expand confituration data requirements and the controls on configuration of serial ports. Beyond serial implications, it could also impact the 4-20 mA inputs (currently in the standard, implications are for routable communications).

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI members who participated in the development of these comments do not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP) and do not support their replacement with the newly proposed term Logical Isolation Zone (LIZ). While there may be future benefits to such a change, this may not be the right time. We are not currently certain that the changes being considered will improve an entity's reliability, security, and compliance efforts through the higher-level objectives set forth by the SDT. Responsible Entities have broadly built their cybersecurity programs around proven concepts, objectives, and programs. The proposed changes will undoubtedly create significant disruption to those systems and efforts. Further, there is concern on the need for such broad changes when there are changes within the body of CIP Reliability Standards that will not be enforceable until the year 2020 (e.g., CIP-005-6). EEI members are also concerned that the level of change being contemplated by the SDT is too great and represents a very steep learning curve for the industry. EEI recommends that the SDT narrow its focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

Logical Isolation Zone poorly defined – because the term "and data" in the proposed BCS Cyber System definition is too ambiguous.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Is it the intent of the SDT that existing ESPs simply convert to a LIZ, where virtual technology doesn't exist? If not, what's the difference between a LIZ and ESP?

We recommend keeping the current ESP/EAP model and the wording in the definitions referencing "routable communication" and "routable protocol connection". In addition, by including serial connected devices in the Requirement, it will require unnecessary additional documentation.

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 no Dominion and NYPA

Answer	No
Document Name	

Comment

Recommend changing the label to clarify this is a security label . . . possibly Logical Security Zones

Audit interpretations of this new, more flexible label are a concern

Concern that this does not enhance cyber security, this is not backwards compatible and forces to re-evaluate what is in scope (ie, microwave communications, serial communications, third party communications, etc). Need better clarification on communications demarcation – what is in scope vs out of scope? Concerned that the current CIP-005 R1.1 has not translated well – need more clarity on establishing boundaries and guidance on how to document

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
MRO concludes that surface area protection architectures such as the Logical Isolation Zone are not necessarily equivalent or a security improvement when compared to existing perimeter protections. Zone or system level protections such as microsegmentation can enhance the protections provided by perimeter protections, but they are not in conflict with each other and can coexist within the same currently defined CIP environment. **The virtualization changes that are proposed will likely permit mixed some trust applications but it isn't yet clear how logical isolation zones will provide better or equivalent protections to that of an ESP.**	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
WAPA does not support the proposed term Logical Isolation Zone (LIZ). "Logical isolation" in computer networking is when two sets of devices, which share a physical network infrastructure, are prevented from being able to communicate with each other. The proposed definition implies that a LIZ is a created by controlling the communications to and from BES Cyber Systems and Protected Cyber Systems. This is the opposite of isolation.	

Logical isolation must distinguish between BES and non-BES. A Logical Isolation Zone could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on common hardware between CIP Applicable Systems and corporate business networks could also introduce risk to the BES.

WAPA recommends using existing, familiar industry terms (as defined in the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298)).

· Replace ESP with NIST's Enclave – A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

· Replace EAP with NISTS's Enclave Boundary – Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a wide area network (WAN).

WAPA recommends the following term be added to the NERC Glossary of Terms instead of LIZ:

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

Likes 0	
Dislikes 0	

Response

7. The SDT is considering taking qualitative language out of the Intermediate System definition and using it to clarify requirements. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Will the Intermediate System extend to the management plane of virtual environments?	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Note: the approach taken requires both the definition and details from the requirements to properly understand the location of the Intermediate System relative to the LIZ and other implications.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
While this change is not related to virtualization, the approach does add clarity to the requirements.	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Button response should be "No". Editing option seems to be broken.

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

This term captures the intent, PAC suggests edits to provide additional scoping keeping Intermediate Systems outside of the Logical Isolation Zone they are designed to help protect:

Intermediate Systems - A [cyber] system acting as part of the protection applied [externally] to a logically isolated BCS that limits external user-initiated access to authorized users.

Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	

We agree with the proposed definition of Intermediate System. We assume that logical isolation is meant to allow policy based access control

A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users.

Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
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	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
Public Power is not sure if this changes the function of the Intermediate System. For example, does the Intermediate System still include the, “jump host concept?” Also, it is not clear if the concept extends to management planes or the actual hypervisor. Clarity on these points would be appreciated. Consider retaining the definition and option to use Intermediate System for entities not pursuing virtualization at this time, and to pilot the new approach with those interested in applying it. This approach will minimize the spread of unanticipated consequences and allow industry and auditors to more gradually learn about the new definitions.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	
abstain	
Likes 0	
Dislikes 0	

Response
Gladys DeLaO - CPS Energy - 1,3,5
Answer	
Document Name	
Comment
Does the IS have to be inside or outside the LIZ?
Likes 0	
Dislikes 0	
Response
James Grimshaw - CPS Energy - 1,3,5
Answer	
Document Name	
Comment
Does the IS have to be inside or outside the LIZ?
Likes 0	
Dislikes 0	
Response
Russell Noble - Cowlitz County PUD - 3,5
Answer	
Document Name	
Comment
Cowlitz supports APPA comment
Likes 0	
Dislikes 0	
Response

David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST. The Intermediate System definition should use “Cyber System” (which needs to be defined) rather than “system.” System is a very broad term and can bring in many devices / equipment currently excluded. In addition, the proposed definition change enables IS to be within the LIZ, which we view as lowering the security bar.	
Likes 0	
Dislikes 0	
Response	

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC does not support the changes being proposed to the term “Intermediate System”, which moves the term from being Cyber Asset based to systems based. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems would be too disruptive to non-virtualization compliance.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST considers the proposed new definition to less clear than the current one, and suggests making only “conforming” changes to the existing definition as needed (such as replacing “Electronic Security Perimeter” with “Logical Isolation Zone”).	
Likes 0	

Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
A missing component of the Intermediate System is the placement of the Intermediate System. Is it the SDT's intention to allow an Intermediate System to reside within a LIZ?	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "EEI does not support the changes being proposed to the term "Intermediate System," which moves the term from being Cyber Asset based to systems based. EEI has significant concerns with this al change because it may provide serious issues for both Responsible Entities trying to develop secure solutions and auditors trying to assess entity compliance with the CIP standards. For this reason, we ask that the SDT consider narrowing their focus to addressing specific issues that might negatively impact an entity's ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed for this informal comment period."	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

The new definition is unclear and requires more analysis.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
This is too vague and needs background before it can be answered.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon does not support this change. The new definition is too broad and may introduce some confusion.	

We ask that the SDT consider narrowing their focus to addressing specific issues that might negatively impact an entity's ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed in this informal comment period.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 7.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
The new definition is unclear and requires more analysis.	
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	No
Document Name	
Comment	

The change to Intermediate System brings into question if the authentication servers used to limit access should be Intermediate Systems as well. Additionally, this language appears to make the location (e.g., inside or outside of the firewall) of the IS ambiguous, whereas the existing definition explicitly states that the IS should be located outside of the ESP.

The existing definition is fairly clear and auditors have a clear approach. Consider retaining the existing Intermediate System definition and add a new "Virtual Intermediate System" definition for those entities that wish to pursue that sort of access.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The Intermediate System definition does not specify that the intermediate system is outside the LIZ. An entity could apply these controls at the BCS level and comply with the standard. The intent is not clear to allow flexibility or require an externally located intermediate system to authenticate users before allowing access to the LIZ and BCS.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does not support the changes being proposed to the term "Intermediate System," which moves the term from being Cyber Asset based to systems based. NV Energy has significant concerns with this projected change because it may provide serious issues for both Responsible Entities trying to develop secure solutions and auditors trying to assess entity compliance with the CIP standards.

For this reason, we ask that the SDT consider narrowing their focus to addressing specific issues that might negatively impact an entity's ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed for this informal comment period.

Likes 0	

Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment
MISO requests clarity on the location of intermediate systems. **Can intermediate systems exist in the same LIZ as other types of CIP Cyber assets, or should they be in a discrete security zone out of a LIZ that contains other types of CIP Cyber assets?**

Likes 0	
Dislikes 0	

Response

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

Comment
Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry. The NSRF does not see the value in changing the definition. We are concerned that by removing the language, "The Intermediate System must not be located inside the Electronic Security Perimeter." could be construed that an Intermediate System could reside inside an ESP or a LIZ.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

Based on our comments on the above, we disagree with the IS definition revisions. The current IS definition is clear and can be applied to the virtual devices as well. As we suggested in the above question 6, the proposed new term LIZ should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol. If SDT wants the IS to apply to LIZ, we suggest revising the IS definition to read (**bold**):

"*A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter* ***or LIZ****.*"

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

The language 'acting as part of the protection applied to a logically isolated BCS…' too broadly scopes the Intermediate System and appears to encompass the definition of an EACS.

Consider changing the proposed Intermediate System (IS) definition to, *A system that limits external user-initiated access to logically isolated BES Cyber Systems for authorized users.* If the SDT does not concur, then BCS to BES Cyber system in the Intermediate System definition should be spelled out.

An Intermediate System is not an applicable system of any CIP requirement. Currently, the EACMS definition includes an Intermediate System in its definition. With the proposed retirement of EACMS the new EACS definition should now say 'this includes Intermediate Systems' in the last sentence of the definition.

Also, the new definition appears to remove the jump-host control from the definition.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Reclamation does not support removing the term Cyber Asset from the definition of Intermediate System. Without “Cyber Asset,” the proposed definition of Intermediate System is too broad.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

Concern that this does not enhance cyber security since the Intermediate System could be on the same sub-net as the BES Cyber System

Does the new definition allow firewalls to be Intermediate Systems?

We do not support the changes being proposed to the term “Intermediate System,” which moves the term from being Cyber Asset based to systems based. We have significant concerns with this change because it may provide serious issues for both Responsible Entities trying to develop secure solutions and auditors trying to assess entity compliance with the CIP standards.

For this reason, we ask that the SDT consider narrowing their focus to addressing specific issues that might negatively impact an entity’s ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed for this informal comment period.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

MEC does not support the changes being proposed to the term “Intermediate System”, which moves the term from being Cyber Asset based to systems based. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004

and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	AZPS Comments - Question 7.docx

Comment

Please see the attached document.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

We do not see the value in changing the definition. We are concerned that by removing the language, “The Intermediate System must not be located inside the Electronic Security Perimeter.” could be construed that an Intermediate System could reside inside an ESP or a LIZ

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The revised definition for Intermediate Systems uses the term “system” which is not formally defined. To be consistent, the definition should follow other terminology changes and include PCS. Recommendation: Use the following definition “A combination of one or more cyber assets acting as part of the protection applied to a logically isolated BCS and/or PCS that limits external user-initiated access to authorized users. Intermediate System components must not reside in the same LIZ as a BCS or PCS.”	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The definition of EACMS included explicit language specifying that an Intermediate System was an EACMS. Explicit language or similar guidance should be provided specifying how an Intermediate System should now be categorized. Should it be considered an EACS? LCRA also supports ERCOT’s comment. A missing component of the Intermediate System is the placement of the Intermediate System. Is it the SDT’s intention to allow an Intermediate System to reside within a LIZ?	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP does not see the value in changing the definition. We are concerned that by removing the language, “The Intermediate System must not be located inside the Electronic Security Perimeter” could be construed that an Intermediate System could reside inside an ESP or a LIZ.

Likes 0	
Dislikes 0	

Response

Jamie Prater - Entergy - 5,6

Answer	No
Document Name	

Comment

NERC Proposed: A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users.

RE Proposed: “A system acting as an intermediatary between protected logically isolated BCS and everything else.”

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Support MRO NSRF Comments

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5

Answer	No
Document Name	

Comment

PSE supports the comments developed by EEI.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO

Answer	No
Document Name	

Comment

Please see MRO NERC Standards Review Forum (NSRF) comments.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy disagrees with the removal of the sentence “The Intermediate System must not be located inside the ESP” from the definition of Intermediate Systems. Was it the drafting team’s intent to remove this phrase, if so, can the team provide its rationale? The concept of Intermediate System has always been understood to mean outside the ESP, but the removal of the language makes this unclear. Also, the proposed definition no longer uses the term “Cyber Asset”, instead uses the term “system”, which seems vague. Can the drafting team clarify what it means by its use of the term “system”?

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

WAPA does not support removing the term Cyber Asset from the definition of Intermediate System. Without “Cyber Asset,” the proposed definition of Intermediate System is too broad.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Southern is concerned that the use of “to” in the Intermediate System definition may limit the ability of shared account access because of an unintentional scoping created by the word “to” implying that we *must* use individual accounts. Southern Company suggests the following revision: “A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access for authorized users only.”

In reviewing the use of “to” and “for”, Southern considered: Does using “to” imply a need for an *account* to be authorized, rather than a *user* being authorized?” and “Will using “to” limit our ability to use shared accounts because of an unintentional scoping created by the word “to” implying that we *must* use individual accounts?”

Southern would also like to ensure that the term “user” in the resulting definition be preserved as this helps clarify *who* we are talking about (i.e. users, not processes).

Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	No
Document Name	
Comment	
The SSRG suggests that the potentially vague vernacular “logically isolated BCS” contained in the current definition of Intermediate System could be replaced with “Logical Isolation Zone (LIZ) for added clarity and cross-definition consistency. Also, the way the new definition is structured, one could construe the Intermediate System can be located within the LIZ. The SSRG suggests adding “The Intermediate System should not be located inside the Logical Isolation Zone” to the definition to maintain consistency with the intent of the original definition.	
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 no Dominion and NYPA	
Answer	No
Document Name	
Comment	
Concern that this does not enhance cyber security since the Intermediate System could be on the same sub-net as the BES Cyber System Does the new definition allow firewalls to be Intermediate Systems?	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

The Intermediate System definition "A system acting as part of the protection applied to a logically isolated BCS..." What kind of "protection?" I think it should specify "logical" or "electronic", etc.

Also, we have concerns about the removal of an “Intermediate System must not be located inside the Electronic Security Perimeter” from the definition of Intermediate System. Does this mean we can have an IS inside an ESP?

The more prescriptive language in the current definition does a better job defining an Intermediate System. We recommend keeping the current definition.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI members who participated in the development of these comments do not support the changes being proposed to the term “Intermediate System,” which moves the term from being Cyber Asset based to systems based. This change may cause serious issues for both Responsible Entities trying to develop secure solutions and auditors trying to assess entity compliance with the CIP standards.

EEI recommends that the SDT consider narrowing its focus to addressing specific issues that might negatively impact an entity’s ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed for this informal comment period.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)

Likes 0	
Dislikes 0	

Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
A missing component of the Intermediate System is the placement of the Intermediate System. Is it the SDT's intention to allow an Intermediate System to reside within a LIZ?	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The proposed new definition implies that if you are using an intermediate system, then you do not have interactive remote access. NRG recommends that the SDT consider leaving the definition as it currently is approved and change the references to the proposed changed terms relating to EACMS.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
While we agree with taking qualitative language of the definition and relocating it to the requirements, we do not believe that the current draft clarifies anything. Instead more questions are raised. For example, an Intermediate System used to have to exist outside the ESP, any ESP. However, can an Intermediate System now exist within a LIZ if it isn't the LIZ of the BCS that it is accessing? Or is this no longer the case and an Intermediate System can now reside within a LIZ? Or, since the Intermediate System is defined as "A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users," does it mean that the BCS at the end of the remote access connection is actually part	

of the Intermediate System and is thus itself part of an Intermediate System? Especially if the BCS had a host-based firewall acting as a LIZ that helped to limit external user-initiated access to authorized users.	
Likes 0	
Dislikes 0	
Response	

8. The SDT is considering changes to the ERC and IRA definitions to address V5TAG issues (see the CIP-005 Technical Rationale document for detailed information). ERC will have conforming changes only and will continue its use as a scoping mechanism. The proposed modifications to IRA will apply to certain non-routable to routable protocol conversion scenarios. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

It is agreed that the revised definition includes the additional intended scope.

The changes to the IRA definition state "...does not include… access initiated from an Intermediate System." It should be made clear in the Intermediate Systems definition that the Intermediate System is an Electronic Access Control System since there is no other clear statement of this. A suggested modification to the Intermediate Systems definition: "An Electronic Access Control System acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users."

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

As long as the conforming changes are so that backwards compatibility remains in place.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees with the changes.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We conceptually agree that IRA should apply to the certain non-routable to routable conversion scenarios (serial to IP)

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
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	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	

Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	
Cowlitz supports APPA comment.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	
abstain	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
Consider dual parallel definitions, existing and new, for these terms, as discussed above.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE does not see a need to change these terms and notes that changing these terms is not specifically related to virtualization.	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
The Technical Rationale continues to use the term, “ESP.” MISO requests that the SDT redraft the Technical Rationale using the new terminology, “LIZ”, to provide clarity.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy does support the changes to ERC, but does not support the change to Logical Isolation Zone at this time, thus defining our No answer for Question 8 at this time. Additional comments on the Logical Isolation Zone are in our response to Question 6. Additionally, NV Energy understands the intent of the revisions to IRA, but it seems that the access initiated from the Intermediate System is treated as similar to system to system access. In adding certain non-routable to routable protocol conversion scenarios into the concept, the SDT should consider this brings in a huge amount of work for entities.	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following: The last clause of the IRA definition “access initiated from an intermediate system” seems contradictory to the intent of using an intermediate system to perform IRA. SDT should consider removing the last clause.	
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	No
Document Name	
Comment	
CHPD agrees that changes may be needed, but the proposed definition is contradictory to CIP-005 R2, which Part 2.1 specifies that it applies to Interactive Remote Access, but the definition of Interactive Remote Access specifies that sessions from the Intermediate System are not considered Interactive Remote Access. Either this is a misunderstanding of the definition and requirement, which means it is confusing, or a mistake in the definition and requirement. Consider removing “or access initiated from an Intermediate System” from the new IRA definition.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	

More work is needed on these modifications.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 8.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon views this change as a step in the right direction to clarify what is and is not an IRA. One concern is how this new definition may bring in non-ERC connections under the new definition. Overall, we do not support the change to Logical Isolation Zone at this time. See comments made in response to Question 6.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
More work is needed on these modifications.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "EEI does not support the change to Logical Isolation Zone at this time. See comments made in response to Question 6."	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	

The modifications to External Routable Connectivity continue to keep the context to being very network centric. This does not address communications that do not use a routable protocol (e.g. fiber channel). This will cause some issues with the implementation of LIZ. Regarding Interactive Remote Access, please clarify the meaning of “access initiated from an Intermediate System”. It is unclear what kind of communication this could be referring to. Please provide clarity on the meaning of “interactive”. Please provide clarity on system-to-system process communication. These have been long-standing issues.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC disagrees with the revisions to ERC and IRA definitions. By removing “with ERC” from the applicable systems column of the requirement tables, multiple requirements will be added to the audit scope that were previously not applicable if there was no ERC. The existence or lack of ERC is fundamental to the current application of CIP Standatrds and removing it will result in additional documentation to prove compliance with no added benefit or reduction in risk.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

In addition, it’s not clear if the proposed change is limited to routable communications or if this intended to also bring serial / other communication mediums within scope of IRA. This requires clarification.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Regarding the proposal to modify the definition of ERC, Duke Energy recommends that the drafting team take this opportunity to provide needed clarity to the concept of routable protocol (i.e. Would serial to IP convertors be included?). The ambiguity around this topic has led to differing interpretations between entities and regulators. Also, modifications to the term IRA, should include some type of clarification on the concept of system to system communications. This continues to be an issue with varying interpretations.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Support MRO NSRF Comments	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA is satisfied with the ERC definition. The IRA definition is contradictory and confusing. CIP-005-7 R2.1 states 'Have one or more methods to ensure that Interactive Remote Access to applicable systems is through an Intermediate System that is isolated from the BES Cyber System and restricts Interactive Remote Access to only authorized users. The definition of IRA states 'User-initiated access by a person employing a remote access client to a BES Cyber System or Protected Cyber System from outside of a Logical Isolation Zone. Interactive Remote Access does not include system-to-system process communications or access initiated from an Intermediate System.' LCRA would also like clarification on the statement 'remote access client…from outside of a Logical Isolation Zone'. Is this intended to mean access from a client outside of any LIZ or only the LIZ that the destination device is associated with? The previous definition of IRA clarified this issue by stating 'not located within any of the RE's ESPs'. The CIP standard states that IRA must be through an Intermediate System, but the definition of IRA states that it does not include access initiated from an Intermediate System.	
Likes 0	
Dislikes 0	
Response	

Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for	

what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

We would agree with the changes if LIZ is replaced with ESP in the ERC and IRA definitions.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	AZPS Comments - Question 8.docx

Comment

Please see the attached document.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

MEC does not support the creation of the new Logical Isolation Zone at this time. Therefore, MEC does not support the proposed changes to the ERC and IRA definitions. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	
Recommend changing from Logical Isolation Zone to Logical Security Zone Concern that this change may bring more Cyber Assets into scope Request more clarity	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support replacing the term Electronic Security Perimeter with the term Logical Isolation Zone (LIZ). Reclamation does not support removing the term Electronic Access Point from the definition of Interactive Remote Access. If a new term for logical isolation is adopted, Reclamation recommends the following be added to the NERC Glossary of Terms: Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

Recommend the SDT remove the word ‘connection’ from the ERC definition to ensure it addresses bi-directional routable protocol access opposed to connection. This is consistent with the SDT’s departure from LERC to ‘using a routable protocol’ in CIP-003-7, Section 3.1, ii.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

Based on our comments on the above, we disagree with revisions of the ERC and IRA definitions. The current ERC and IRA definitions are clear and can be applied to the virtual devices as well. As we suggested in the above question 6, the proposed new term LIZ should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol. If SDT wants the IRA to apply to non-routable for the LIZ, we suggest revising the IRA as follows (**bold**):

“User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol **to pass through ESP or non-routable protocol to pass through LIZ**. 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), LIZ or at a defined Electronic Access Point (EAP). 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. Interactive remote access does not include system-to-system process communications.”

If SDT wants the ERC to apply to LIZ, we suggest revising the ERC as follows (**bold**):

The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter **or LIZ** via a bi-directional routable protocol connection.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is

recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

The non-routable definition is fundamental to the current understanding and application of CIP standards.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

BPA proposes changing the ERC definition:

Current Proposed: "External Routable Connectivity" is the ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Logical Isolation Zone via a bi-directional routable protocol connection.

BPA Proposed: "External Addressability" is the ability to direct communications traffic to a BES Cyber System from cyber systems external to an entity's Logical Isolation Zone.

BPA believes this change adequately mitigates the risk of what was formerly known as ERC and allows the scope of controls to exclude communications between secure Logical Isolation Zones. Communications originating inside an LIZ and proceeding to another LIZ are already protected and do not pose additional risk to applicable systems. BPA's proposed change provides better alignment with IRA requirements and retains better backward compatibility with the current ESP model.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

This term captures the intent, seems that the access initiated from the Intermediate System is treated as similar to system to system access. In adding certain non-routable to routable protocol conversion scenarios into the concept, the SDT should consider this brings in a huge amount of work for entities. PAC would request a 24 to 36 months implementation period for the changes proposed by these revisions.	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
PGE doesn't see that the proposed change in definition have resulted in the desired scope change being applied. Is the proposed definition meant to incorporate the change outlined above? PGE agrees that those types of Interactive Remote Access could benefit from additional security controls.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
The conforming changes for ERC appear to be acceptable. However, if nested LIZ are allowed then consider changing "Logical Isolation Zone" to "Logical Isolation Zone(s)". As for IRA, the proposed changes had setup a dichotomy regarding the protection paradigm of CIP. If user-initiated access by a person employing a remote access client to a BCS or PCA from outside a LIZ, then it appears any access initiated from any LIZ regardless of impact level is acceptable. However, the drafted CIP-005 R3 proposes that further restriction between the data plane and management plane is required. So why is it acceptable to allow any LIZ to LIZ traffic and yet restrict the management plane and data plane? It appears the CIP-005 R3 is accomplished with a LIZ around the management plane. Yet IRA allows LIZ to LIZ traffic, so a CIP paradox has been created and more ambiguity regarding what is allowed and not. This would make the proposed IRA change and proposed requirement changes difficult to audit.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	

Answer	No
Document Name	
Comment	
Not clear whether IRA will apply to non-routable to routable protocol conversion scenarios.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
When you remove ERC, you eliminate a threat vector to the ESP. Therefore, the controls required in that situation should reflect that. This proposed standards change reinstates a lot of the controls that were not required under the current version of the standards, which could cause a compliance burden to the industry that may exceed the risk mitigation acheived. NRG asserts that the proposed definition changes to IRA may contradict the requirements relating to CIP-005. The new IRA definition specifically describes that IRA does not include sessions initiated from an intermediate system. As written, registered entities using an Intermediate System, are excluded from CIP-005 R2.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The modifications to External Routable Connectivity continue to keep the context to being very network centric. This does not address communications that do not use a routable protocol (e.g. fiber channel). This will cause some issues with the implementation of LIZ. Regarding Interactive Remote Access, please clarify the meaning of “access initiated from an Intermediate System." It is unclear what kind of communication this could be referring to. Please provide clarity on the meaning of “interactive." Please provide clarity on system-to-system process communication. These have been long-standing issues.	
Likes 0	
Dislikes 0	

Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
Not clear whether IRA will apply to non-routable to routable protocol conversion scenarios.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The EEI members who participated in the development of these comments do not support the change to Logical Isolation Zone at this time. See comments made in response to Question 6.	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
In our opinion LIZ is not a good replacement for ESP. The proposed definition for LIZ doesn't define "communications" or "controls" and results in a definition that is too vague. We recommend keeping the term ESP in lieu of LIZ.	
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 no Dominion and NYPA	
Answer	No
Document Name	
Comment	
Recommend changing from Logical Isolation Zone to Logical Security Zone Concern that this change may bring more Cyber Assets into scope Request more clarity	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	No
Document Name	
Comment	
The SSRG proposes that “system-to-system process communications” should be a defined term that mitigates subjectivity across the industry and provides an objective basis for compliance; and suggests the following definition for “System-to-System Process Communications” could be incorporated: “System to system process communications are communications that are not intiated by a user, but directly by a system to another system with no human interaction.”	
Likes 0	

Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

User-initiated access by a person employing a remote access client to a BES Cyber System or Protected Cyber System from outside of a Logical Isolation Zone. Interactive Remote Access does not include system-to-system process communications or access initiated from an Intermediate System. Southern requests the SDT consider adding “or other remote access technology using a routable protocol” back in to the definition to retain proper scoping. We do not want KVMs and similar “dumb devices” to be unintentionally scoped in.

Southern would also like clarification on the definition for Interactive Remote Access. While the inclusion of “by a person employing a remote access client” helps clarify that we are discussing people using accounts, this is also implicitly stated later in the definition. Also, including “remote access client” implies that the remote access software be client based and we feel that excluding this will help clarify the scope of the definition.

We propose the following as an alternate IRA definition:

“User-initiated access to a BES Cyber System or Protected Cyber System from outside of a Logical Isolation Zone. Interactive Remote Access does not include system-to-system process communications or access initiated from an Intermediate System.”

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

WAPA does not support replacing the term Electronic Security Perimeter with the term Logical Isolation Zone (LIZ).

If a new term for logical isolation is adopted, WAPA recommends the following be added to the NERC Glossary of Terms:

· Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

Likes 0	
Dislikes 0	
Response	

9. To the extent possible, the SDT intends its modifications to permit approaches to compliance that are "backwards compatible" with compliance approaches within the currently approved versions of the CIP standards. (Notable exceptions include CIP-005 R3, CIP-007 R2, and Secure Configurations – CIP-010). Do you agree the modifications are backwards compatible? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Nicholas Lauriat - Network and Security Technologies - 1

Answer	Yes
Document Name	

Comment

N&ST notes that Responsible Entities with no virtualization or limited (no "mixed trust") virtualization would still be compelled to make extensive (and possibly time-consuming and/or costly) to their CIP evidence files.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES

Answer	Yes
Document Name	

Comment

We agree that the changes appear to be backward compantible, however there are a lot of questions at this point of how comliance will be assessed, especially as we move away from assets toward systems.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	Yes
Document Name	

Comment

Not all entities have adopted virtualization therefore, it is important that terms and concepts remain separated to avoid confusion where there is clearly a separation of physical and virtual environments.

Likes 0	

Dislikes 0	

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	

Comment
The “ERC” qualifier has been removed from CIP-007 R1.1. This could dramatically increase burden on some entities, where the intended effect could be achieved instead with a virtualization-ready definition of “PCA” and “ERC.” CIP-007 R1.4 also seems to shift from requiring intrusion protection on an ESP level to requiring it on a BCS level. This will be onerous and may not be technical feasible in many cases, unless BCS are defined over-broadly (i.e., the entire LIZ is a single BCS). There is a meaningful distinction in keeping the BCS definition separate as a subcomponent of the LIZ. The appropriate shift would be from EAP to LIZ, not from EAP to BCS.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	

Comment
: NOTE: All references to the new definitions need to be addressed in all the Standards I.e. CIP-009-6 references EACMS an term now being split into EACS and EAMS.

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment
PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
The modifications are backwards compatible, and will proide an increase in security, but they will create more work as the Secure Configuration covers more areas than the current Baseline Configuration.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
The modifications are backwards compatible, and will proide an increase in security, but they will create more work as the Secure Configuration covers more areas than the current Baseline Configuration.	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
PGE has not completed a detailed requirement by requirement analysis but generally believe that these proposed standards provide backwards compatibility.	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
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	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	

Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No position. No comment.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
Because of the extensive changes to both definitions and Standards, and as a yet-to-be- determined audit approaches, it is not possible, at this time, to be certain that the modifications are indeed backwards compatible. As an alternative that better assures backwards compatibility, consider the option to retain the existing definitions and requirements along with instituting the new definitions and requirements, and then direct entities to select among these two options, on a cyber system basis. This option could be planned to sunset after a set number of years.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	

Answer	
Document Name	
Comment	
abstain	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE suggests these changes are not necessary as they do not specifically relate to virtualization. These changes appear to be wholesale changes and vastly change the approach of the CIP Standards. Industry just recently went through a large change with the implementation of CIP version 5.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No

Document Name	

Comment

SMEC appreciates the intent of backwards compatibililty, but the proposed changes will not be backwards compatible for existing compliance documentation. The proposed changes (i.e., removing ESP/EAP, removing BES Cyber Asset definition, etc.) will require entities to change documented processes and compliance evidence for multiple CIP standards. As suggest before, the proposed new term LIZ should only apply to the virtual devices while keeping the existing requirements the same as before. Another alternative would be a new standard which applies only to virtualized systems to address related concerns, thus adding no burden to those entities without virtualization.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

The definition of Secure Configuration is recursive and incomplete. The applicability to specific language should not be included in the definition.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"EEI is concerned with the broad changes being contemplated by the SDT. While we applaud the SDT's effort to make these changes "backward compatible" with existing systems not operating within a virtualized environment, the proposed changes system approach introduces new risk to security. We are also concerned that the changes being considered do not take into consideration that the vast majority of systems do not operate within a virtualized environment and are unlikely to be moved in that direction anytime soon. The industry needs more time to better assess the potential disruptive impacts given there are no pressing needs for such changes. More importantly, we cannot say with confidence that the modifications proposed are clearly backward compatible and do not create unintended problems that might compromise BES reliability and security.

EEI recommends that the SDT to narrow the focus of this effort to provide clear implementation guidance to protect BES Cyber Systems within virtualized environments under the existing framework already in place."

Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
We see that a LIZ can be backwards compatible to as ESP, but other changes are not backwards compatible.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
For the most part the current draft presents a systematic approach which is backwards compatible, but Cyber Assets are discrete objects which cannot be systematically removed unless replacing the entire Cyber System. Further CIP-011 contains the term Cyber Asset for disposal and reuse. CIP-011 needs to be modified or further delineation in the BCS definition due to the fact that Cyber Assets, virtual or physical, are still discrete parts of a BCS and cannot be handled systematically.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

Even with the “proposed backward compatibility,” this change will be disruptive to current CIP programs in place, requiring documentation, compliance tool/technology and process changes. Major changes to our CIP program would be required just to address the foundational definition changes, CIP-002 methodology and assessments, device and asset inventory, patching and change management tools, as well as the entire suite of program, process and procedural documents.

We cannot say with confidence (within this comment period) that the modifications proposed are clearly backward compatible and do not create unintended problems that might compromise BES reliability and security. The proposed changes bring with them a very steep learning curve for the industry.

The timing and scope of these changes is concerning, as they represent a major overhaul of the CIP Standards. We would prefer for the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 9.

Additionally, Westar | Kansas City Power & Light Company share the following concerns.

Recognizing the issue that is being addressed, the strategy “backwards compatible” is ripe with compliance ambiguity and confusion.

The Standards or their revisions are approved and effective at a point in time. That required certainty as to when a Standard is effective is fundamental to compliance and, for that matter, auditability.

Any compelling need to consider “backwards compatibility” can be addressed in Implementation Plans or revisions to the specific Standard. Attempting to address globally will not serve compliance and, in turn, reliability.

Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
We see that a LIZ can be backwards compatible to a ESP, but other changes are not backwards compatible.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
The extensive changes to definitions significantly interferes with practical implementation of the standard in a backward compatible manner. While on the surface, the changes appear to be capable of being backwards compatible, significant research through a detailed study program is required. Unfortunately, this requires time and the standards are far behind the technology and the increased reliability the new technology provides. A certain component of the backward compatibility will need to be taken on faith. This will need to include modified definitions and guidance that is publicly accepted by NERC as valid. Clear guidance needs to be created that virtualization that is not mixed mode continues to meet the requirements.	
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	No
Document Name	
Comment	

CHPD is concerned with how this question is asked. The question essentially asks “other than the proposed changes, is the SDT’s proposal backwards compatible?” The Secure Configuration concept is such a large deviation from the existing standards that we believe is not valid to exclude it from a question like this. No entity would be able to carry their existing program forward given the sweeping changes proposed, even if they do not intend to virtualize.

The changes to EACMS (splitting into EACS and EAMS) do seem to be largely backwards compatible, so long as you exclude the proposed Secure Configuration concept.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The proposed CIP-010 language does not address a compliant way to authorize changes after the fact. Previous Requirement R1.2 required change authorization without requiring a timeframe, after the change if necessary. This could be due to operational necessity or minor administrative delay. The new language does not have this flexibility.

The new CIP-007 language requires baselining of all executable scripts. Scripts and “custom” software have been a poorly defined area, but the language in the new standard is broad and therefore difficult to implement or enforce given that any user can enter, execute, and delete scripted commands at a shell prompt. The underlying intent of CIP-007 is a good one, but entities must have the flexibility to automate administrative processes on their own systems, planned or ad-hoc. Furthermore, while installed software or packages are recognized by the OS and can therefore be monitored, scripts are not installed and may not even exist as files. Baselining or alerting on scripts is not practicable.

The new CIP-007 language also requires provision of only “essential” logical access and “essential” software. This is a strong and undefined term. Entities must flexibility to determine what is needed and to revise their determination as their system, or understanding of the system, evolves over time. Language in the new CIP-007 Requirements R1.1 and R2.1 provides no flexibility in revising what is “essential” in a compliant way. CenterPoint Energy recommends that the SDT provide clarification and more context around the term “essential.”

Malicious code deterent, detective, or preventative controls may be external to a BCS that cannot run host-based anti-malware controls and therefore cannot be part of the Secure Configuration of the BCS. The NOTE about Secure Configuration should read “The implemented configuration, where implemented on the applicable System, in support of this Part becomes part of the Secure…..”

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	
Comment	

NV Energy would like to praise the SDT's effort to make these changes "backward compatible" with existing systems not operating within a virtualized environment; however, the proposed changes system approach introduces new risk to security. We are also concerned that the changes being considered do not take into consideration that the vast majority of systems do not operate within a virtualized environment and are unlikely to be moved in that direction anytime soon. The industry needs more time to better assess the potential disruptive impacts given there are no pressing needs for such changes. At this time, NV Energy cannot say with confidence that the modifications proposed, are clearly backward compatible and do not create unintended problems that might compromise BES reliability and security, as this will require additional time and analysis to determine.

NV Energy recommends that the SDT to narrow the focus of this effort to provide clear implementation guidance to protect BES Cyber Systems within virtualized environments under the existing framework already in place.

Likes 0	
Dislikes 0	
Response	

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	
Comment	

MISO does not agree that the changes are backwards compatible. However, MISO recognizes the need for Standards to change as threats evolve and supports the direction of the SDT. Providing clarity regarding the changes and recommendations for proper implementation will facilitate a smoother transition.

Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	
Comment	

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

The SDT did a good job here. PAC disagrees with the EACMS and PACS changes and believe we can accomplish the same without the new terms.	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP agrees with modification of Requirements to reduce barriers for increased flexibility and to allow application of new thechnology. However, AEP believes the change from Configuration Baseline to Secure Configuration and additional requirement for risk assessment exceed the mandate from the SAR and will be an unnecessary burden to Industry.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry. The NSRF feels there will be significant changes to required documentation. The MRO NSRF has further concerns the proposed revisions change how to comply but don't improve system reliability or security. The relatively quick timeframe in which these significant proposed changes were made presents the risk of many unintended consequences for what is the vast majority of systems that are not in virtualized environments. The NSRF agrees that there is a need to take a different approach to Cyber and Physical Security of the Bulk Electric System, however with the continuous state of change and adjustments being made to NERC CIP requirements we do not feel that this is the proper project to take on a larger transformational change.	

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	
The same comments as the above question 6. Given that the CIP compliance process today works fairly smoothly by applying the existing requirements that are appropriately prescribed, any backwards compatible changes have no value for the CIP compliance but wasting the entities' resources for make these changes.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
There are two types of "backwards compatible" – technological and documentational. For entities not employing virtualization, there should be no need to update either the documents or the technologies that refer to ESP and other existing terms. The proposed changes (i.e., removing ESP/EAP, removing BES Cyber Asset definition, changes to EACMS/EACS/EAMS/PAMS/PACS, etc.) will require *all* entities to change their documented processes and compliance evidence for the entire suite of CIP standards.	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	

We do not agree that the changes are backwards compatible since existing policies / procedures (system changes, patch management, re-labeling equipment, etc) may need to be re-written and staff will need new training. One example is changing EAP to Logical Security Zone.

Fundamental changes to protection controls which were established CIP Standards version 3.

We are concerned with the broad changes being contemplated by the SDT. While we applaud the SDT's effort to make these changes "backward compatible" with existing systems not operating within a virtualized environment, the proposed changes system approach introduces new risk to security. We are also concerned that the changes being considered do not take into consideration that the vast majority of systems do not operate within a virtualized environment and are unlikely to be moved in that direction anytime soon. The industry needs more time to better assess the potential disruptive impacts given there are no pressing needs for such changes. More importantly, we cannot say with confidence that the modifications proposed are clearly backward compatible and do not create unintended problems that might compromise BES reliability and security.

We recommend that the SDT narrow the focus of this effort to provide clear implementation guidance to protect BES Cyber Systems within virtualized environments under the existing framework already in place.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We appreciate the intent of backwards compatibility, but are not convinced this will work with the security objective-based requirements subject to different interpretations by Responsible Entities and auditors. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the "how to comply" with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

We disagree that the changes are fully backwards compatible in compliance approach as CIP-004 now includes an access control program for PCS (PCA). There may be many PCA devices within a substation that must be added to the access control program which may require changes to the compliance approach. This may require changes to PCS/PCA controls to bring them into the CIP user authorization program

We do agree that the majority of the changes are backwards compatible from a compliance/ controls approach, but will require extensive documentation changes.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS does not agree that all changes are “backwards compatible” as the proposed modifications are expansive and it is, therefore, difficult to determine with certainty if the changes will generally be backwards compatible. It is also likely that changing definitions that are used throughout all CIP standards will have impacts beyond those immediately obvious, and could affect internal controls.

As an example, AZPS believes the following changes will not be “backwards compatible” and may require extensive changes to internal programs:

- Removal of the term BCA. AZPS has structured its CIP environment to be processed at the BES Cyber Asset level. While AZPS agrees that moving to a BES Cyber System level is appropriate, it will require extensive changes for AZPS to conform its program approach, associated documentation and work processes, associated technology, etc.
- Removal of “routable protocol” from the definition of IRA. This will increase the scope of devices for which compliance with the CIP reliability standards is applicable. Further, this change creates inconsistency by continuing to use “routable protocol” in the applicability tables.

For these reasons, there is a high likelihood that the proposed changes are not wholly backwards compatible and would require a significant effort to revise and implement.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	
Comment	

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

We feel there will be significant changes to required documentation.

Likes 0	
Dislikes 0	
Response	

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	

SRP does not agree the modifications are backwards compatible due to the expansion of applicability for various requirements. For example, under the proposed requirement updates, the applicability for CIP-004 R3, R4, and R5 would extend to PCS. If the requirement did not previously apply to certain systems, and the SDT is not following a FERC Order to expand the scope, then SRP does not see a need to expand the applicability of the requirements. In addition CIP-005 R1.2.1 is not backwards compatible as it brings serial port connectivity in scope of the standard and also may indirectly imply encryption on the connections.

Additionally, SRP believes removing the term 'routable protocol' from the definition may bring serial connections in scope, which are currently excluded. Not excluding serial connection does not allow for backwards compatibility.

SRP also agrees with the comments by APPA.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

Support MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

It is difficult to answer the question of backwards compatibility without gaining the necessary clarity on some of the definition proposals. Having said that, it appears at first glance, that certain programmable devices that are considered non-CIP devices (Variable Frequency Drive), would now be considered CIP based on some of the proposed changes. If that is the case, we fail to see how this would equate to backwards compatibility.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Southern Company notes concerns with “logical connectivity” in CIP-007 R1.1 below in Q14.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer	No
Document Name	

Comment

1.) On its face, the SSRG believes the proposal will require significant documentation and system changes to implement and is concerned the modifications are not truly backwards compatable with the current baseline. The SSRG requests the drafting team clarify or explain what the Secure Configuration includes that is not part of the original baseline configuration.

2.) Does the standard drafting team intend the “baseline” paradigm of CIP-010-3 R1.1 to be congruent (i.e., “backwards compatable”) with the new “Secure Configuration” paradigm documented in the proposed CIP-010-4 R1.1? In addition, are the controls as documented in CIP-010-4 R1.1.2 indended to be the same as controls as documented in CIP-010-4 R1.2.1. If yes, to avoid confusion and provide specificity to the requirements, the SSRG suggests utilizing corresponding or parallel language in each section where appropriate.

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 no Dominion and NYPA	
Answer	No
Document Name	
Comment	
We do not agree that the changes are backwards compatible since existing policies / procedures (system changes, patch management, re-labeling equipment, etc) may need to be re-written and staff will need new training. One example is changing EAP to Logical Security Zone. Fundamental changes to protection controls which were established CIP Standards version 3.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
With all the additions, deletions, and revisions to so many terms and definitions it is not possible at this time to be sure of backwards compatibility.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
While the changes appear to be relatively backwards compatible, the items that are required to be part of the Secure Configuration in effect expand the scope of what is required for change control (per CIP-010 R1) in a non-virtual environment. For this reason, we believe the modifications do not appear to be entirely backwards compatible. Tri-State would like to request additional guidance to include an example and a graphic of how backwards compatibility would look for each of the changes.	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI members who participated in the development of these comments are concerned with the broad changes being contemplated by the SDT. These members applaud the SDT's effort to make these changes "backward compatible" with existing systems not operating within a virtualized environment; however, the proposed changes may introduce new risk to security. There is concern that the changes being considered may not take into consideration the vast majority of systems that do not operate within a virtualized environment and are unlikely to be moved into such an environment soon. For these reasons, more time may be needed to better assess the potential disruptive impacts given there are no pressing needs for such changes. As stated earlier, it is not clear that the modifications proposed are clearly backward compatible and concern that the proposed modifications do not create unintended problems and consequences that might compromise BES reliability and security. To address these concerns, EEI recommends that the SDT focus first on providing clear implementation guidance to protect BES Cyber Systems within virtualized environments under the existing framework already in place.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	

Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The definition of Secure Configuration is recursive and incomplete. The applicability to specific language should not be included in the definition.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
NRG disagrees with this proposed change because it would cause registered entities to re-assess all aspects of their current NERC CIP compliance programs. An entity cannot be backwards compatible and also achieve the newly proposed requirements. The new secure configuration definition mandates malware monitoring within BES Cyber Systems which implies AV on the BCS and not at the system level (which is the only requirement of the current standard). This proposed change could also imply needing network access control, whitelisting, and/or needing host based intrusion detection.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	

Answer	No
Document Name	
Comment	
PNMR agrees with EEI's comments. Thank you for attempting to make the changes "backwards compatible." However, due to the number of definition changes along with requirement changes there are several unintended consequences. Our responses to other questions have brought up only some of the ones that we have identified so far.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Improvements are needed to assure backwards compatibility is retained.	
Likes 0	
Dislikes 0	
Response	

10. The SDT has not yet determined a proposed timeframe to include in the Implementation Plan. How long would you as an entity need to implement the proposed modifications? Please provide your implementation timeframe and justification for why that amount of time would be needed.

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	
Document Name	

Comment

An implementation period would largely be to update documentation and not change technical implementation. A period of 6 months would be sufficient if backwards compatibility is maintained, 12 months minimum for technical implementation changes.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	
Document Name	

Comment

2 to 5 years

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	
Document Name	

Comment

We hesistate to provide an estimate and justification for an Implementation Plan, without gaining the clarity on some of the proposed terms.

Likes 0	
Dislikes 0	

Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
MISO suggests an implementation period of 3 years; the SDT may find it appropriate to design a phased-in implementation with LIZ being in the earlier waves of implementation. Specifically, MISO urges the SDT to clearly define "secure configuration" and/or provide additional guidance on the concept.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	
Document Name	
Comment	
We appreciate the SDTs effort to make the updated requirements backwards compatible but even for an entity that has no virtualization the updated requirements and terms will necessitate re-evaluation of assets, updates to policies and procedures, and implementation of new controls and concepts (for example, the Secure Configuration concept). Based on this alone, we believe that 24 months would be the minimum timeframe required to implement the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	

This Project has made a substantial amount of revisions to the existing CIP Standards, which in turn will require significant overhaul of existing programs and documentation, and at minimum, should require the same implementation timeline that was provided for the CIPv5/v6 implementation.

NV Energy would request a 24 to 36 month timeline for implementation if these revisions are approved.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

18 to 24 months at a minumum. There is great deal of change that will have to be considered, created, and then implemented. The idea presented by some others on phased implementation similar to what was done for V5 also has some merit if it can explained clearly how it can be used and the Regions are willing to accept it.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

CenterPoint Energy suggests the Implementation Plan to be 24 months after Federal Energy Regulatory Commission (FERC) approval. The proposed changes to address virtualization and emerging technologies is significant and a major overhaul of the standards. Entities need sufficient time and resources for implementation and documentation.

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	
Document Name	

Comment

Given the sweeping changes being proposed, CHPD cannot see an implementation period of any less than 36 months. The additional inventory required as part of the Secure Configuration would require this. Additionally, CIP-005 R3 would require network architecture changes that would not be simple to implement.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	
Document Name	

Comment

Not only will this implementation require adaptation to the new standard, but also restructuring of existing systems with new terminology and re-evaluation of BES Cyber System categorization. This is a widely variable time period depending on size of company. An appropriate implementation plan must allow some type of flexible adoption of the revisions depending on the network and systems considered.

For example, an entity not using virtualization may choose to adopt the new standard at a single point in time when language in their systems have been changed. Other entities that are currently using virtualized systems may adopt the new compliance standard at various times for each logical isolation zone that contains virtualized systems.

At a minimum, two years will be required at large entities. The radical changes in the standard will cause smaller entities to delay work until the standard is approved by FERC, unless FERC provides some kind of feedback that approval is expected. Again, two years would be the minimum time frame to consider.

Likes 0	
Dislikes 0	

Response

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6

Answer	
Document Name	

Comment	
18 months	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	
Document Name	
Comment	
CIP-005 changes could require extensive architectural changes. This would impact budgets,hardware, software and respective life cycles typically plan three year out. Likewise, The secured configuration management proposed changes could take many years to design and implement. The proposed changes for EACS/EAMS and PACS/PAMS could be implemented much more quickly with tangible benefits within a year. Likewise, the vulnerability management change could also be implemented relatively quickly.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 10. Additionally, Westar | Kansas City Power & Light Company supplements the EEI response with the following detail: A minimum of three years, likely longer in some instances, to implement the proposed strategy. To address the proposed revisions / additions to the CIP Standards will require: • complete review of all systems; • likely investment in additional or upgraded cyber assets; • training; • potentially adding or contracting scarce cyber security engineering expertise; and • wholesale revision to the company's CIP processes and procedures.	

The proposed strategy will be a substantial undertaking regardless of an entity's size.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	
Document Name	

Comment

Due to concerns stated above, Exelon does not support the timeframes included in the Implementation Plan. A company of our size needs a minimum of three years to make major changes to our CIP program. One year to understand the requirements, agree on a direction for our program and get financing in place; 18 to 24 months to establish the project and deliver; 3 to 6 months to execute, monitor and adapt prior to the compliance enforcement date.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

18 months

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	
Document Name	

Comment

We are asking for a 48 month period to implement the proposed modifications. This would allow for programmatic alignment to be accomplished during review cycles, documentation alignment and review, and additional time to align process and procedures.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	
Document Name	

Comment

CIP-005 changes could require extensive architectural changes. This would impact budgets,hardware, software and respective life cycles typically plan three year out. Likewise, The secured configuration management proposed changes could take many years to design and implement.

The proposed changes for EACS/EAMS and PACS/PAMS could be implemented much more quickly with tangible benefits within a year. Likewise, the vulnerability management change could also be implemented relatively quickly.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"Due to concerns stated above, EEI does not support the timeframes included in the Implementation Plan."

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	
Document Name	

Comment

24 months is needed at a minimum. Entities need to reevaluate technologies currently used to manage processes supporting compliance to the requirements. This is particularly important with transitioning from patch management to vulnerability management. This will most likely require capital investments which require adequate budget time.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES

Answer	

Document Name	
Comment	
24 months.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	
Document Name	
Comment	
N&ST believes the proposed modifications represent a significant change to the CIP Standards. Based on that opinion, N&ST believes the implementation time frame should, if all proposed modifications were approved, be at least 24 months.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	
Comment	
3-5 years	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	

Twelve months as the proposed changes are backwards capatible and our current protections for virtualized systems align perfectly with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	
Document Name	
Comment	
PSE supports the comments developed by EEI.	

Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
Support MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	
Document Name	
Comment	
3-5 years	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP recommends including an additional 36 to 48 months in the Implementation Plan because the new terminology and retired terminology are now in more requirements creating a review and revision administration burden. This will allow Responsible Entities time for planning, budgeting, and evaluating new tools, hardware, software, professional services, architectural changes, and encryption.	

Additionally, the suggested changes increase the scope substantially by including serial connectivity and applicable devices into requirements they were not previously in. This is an overhaul of the CIP standards just as with version 3. SRP also requests the time frame between the current standards and the standards with the revised methodology be treated as the CIPv3 to v5 transition. SRP also agrees with APPA's comment regarding a pilot program.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
LCRA proposes a 24 calendar month timeframe to implement the proposed changes. Some changes to the standards, such as those related to Secure Configuration, will require testing on how to best implement the requirements for LCRA's BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	
Document Name	
Comment	
3-5 years would be required to address (document, fund and implement) significant changes to systems that will support the new requirements (i.e. CIP-007 R2).	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	
Document Name	

Comment
18 - 24 calendar months. This would allow entities time to redo their processes and properly address the risk based language that has been included. It would also allow some technical changes to occur for new or revised requirements (i.e. data communicaiton encryption, etc.). Additionally, it would be beneficial to have the option for entities to adopt the revised requirements early, once approved by FERC, similar to how CIP Version 5 was implemented.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	
Document Name	

Comment
NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations. We do not agree with most of the changes, especially the removal of BCA and ESP. If the changes were to go through as proposed we would request a minimum of 24 months due to architecture redesign, documentation updates, and documentation review.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	

Comment
AZPS respectfully requests consideration of a 30-month implementation plan timeframe given the wide breadth of change required.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Three years because this change is similar in scope to upgrading from CIP version 3 to 5. We suggest borrowing from that earlier implementation plan, where each Entity had the option of which version to adhere to and by BES Cyber Asset / BES Cyber System (instead of wholesale conversion).	
Likes 0	
Dislikes 0	
Response	

Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
We propose a three years timeframe since this change is similar to when CIP version 3 was upgraded to version 5.	
Likes 0	
Dislikes 0	
Response	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
If NERC and FERC approve such wide-sweeping changes, industry will need at least as much implementation time as was provided for CIP version 5 to overhaul all CIP programs and retrain personnel and practice on all standards before the effective date. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the	

existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	
Document Name	

Comment

Three years because this change is similar in scope to upgrading from CIP version 3 to 5.

We suggest borrowing from that earlier implementation plan, where each Entity had the option of which version to adhere to and by BES Cyber Asset / BES Cyber System (instead of wholesale conversion).

Likes 0	
Dislikes 0	

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC

Answer	
Document Name	

Comment

Two years. As described elsewhere in this response, the proposed changes blur the line between what constitutes a Logical Isolation Zone and a BES Cyber System, now applying Requirements at the BCS level that previously applied only to an EAP or an ESP with ERC. Depending on the system, these changes could require a combination of major technical enhancements on a BCS level and the administrative burden of restructuring what constitutes a BCS. The changes could be more backward-compatible, and therefore faster to implement in most cases, if network-level protections are applied to the Logical Isolation Zone while system-level protections are applied to the BCS. The proposed isolation of the Management Plane from the Data Plane could be more backward-compatible if its application scope is refined to only those assets where the Management Plane would be capable of changing the isolation limits or accessing internal data from outside of a Logical Isolation Zone, for which we propose the new term “Zone Boundary System.”

Likes 0	

Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation recommends the SDT consider separate, 24-month phased-in implementation plans for each affected CIP standard to avoid numerous changes becoming effective on the same date. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel appropriately. Reclamation suggests the SDT consider a longer implementation schedule for entities that use virtualization (e.g., an additional 18 months) than for those that don't.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
Minimum 24 months. Entities are adapting to the new terms and mapping backward compatibility. The terms used require piloting in operational environment to highlight implementation difficulties. The extra time also smothes out work burden to avoid overload of existing staff levels.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	

Comment
18 months is needed to ensure….

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	
Document Name	

Comment
We disagree with most of the proposed changes except EACMS and PACS.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment
Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There is also multiple registered groups who can write and submit to NERC, Implementation Guidance. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtuazation practices under our current set of Standards. All Standards are written to “what to do” not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still do not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry. We do not agree with most of the changes, especially the removal of BCA and ESP. Industry needs 4 calendar years or 48 months to adequately design, spec, budget, build, implement, rewrite program documents and train on all of the new requirements. Each one of these phases takes time to implement.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA points out that with the definition changes it will be impossible to utilize a phased implementation approach; therefore we predict a long implementation period will be necessary for most entities. Transition to the new version should be allowed prior to mandatory and enforceable date.	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	
Document Name	
Comment	
AEP believes systems changes and process changes to account for classifications and changes to definitions would require at least 24 months to implement or longer if requirements to assess risk as proposed in CIP-010-4 are retained.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
: PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. PAC would request a 24 to 36 months implementation period for the revisions proposed.	
Likes 0	
Dislikes 0	
Response	

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	
Document Name	
Comment	
2-5 years due to small public entities with limited staff and resources. These entities must first budget through the approved budget that is not as fexible as larger agencies. This includes public meetings and voting by publicly elected officials. Typically, one FTE is a significant expense and must be well supported. Additonal systems, equipment and processes take considerable resources in small organiztions. Repetative work loads must also me considered for staffing purposes at smaller agencies. Physical and Cyber Security has been one of the single bigest cost drivers in small agencies and has begun to negatively impact rural ratepayers, especially in depressed economies that still struggle to get basic services.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have a comment on this question.	
Likes 0	
Dislikes 0	

Response
Russell Noble - Cowlitz County PUD - 3,5
Answer	
Document Name	
Comment
Cowlitz supports APPA coments.
Likes 0	
Dislikes 0	
Response
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro
Answer	
Document Name	
Comment
BC Hydro’s assessment is that, due to the scope of this assessment on the BC Hydro systems, at least 24 calendar months would be required to analyze the full impacts of the proposed modifications.
Likes 0	
Dislikes 0	
Response
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6
Answer	
Document Name	
Comment
PGE would propose a minimum of 24 months for implementation of the new standard. PGE would also suggest guidance for entities and auditors alike on how to make the transition as seamless as possible. The ability to transition early for those entities that wish to take advantage of the flexibility allowed in the standard should be addressed.
Likes 0	
Dislikes 0	

Response
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3
Answer	
Document Name	
Comment
It is unclear if the proposed modifications could even be successfully implemented to be auditable with just some of the concerns raised in our other comments. Without more time to process these changes and ramifications, we cannot even guess as to how long we would need to implement the proposed modifications.
Likes 0	
Dislikes 0	
Response
James Grimshaw - CPS Energy - 1,3,5
Answer	
Document Name	
Comment
2 years (budgetary reasons, training, reconfiguration of systems, compliance with Secure Configuration, risk analysis, etc.)
Likes 0	
Dislikes 0	
Response
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF
Answer	
Document Name	
Comment
NRG asserts that registered entities would require at least 24 months to implement these technical changes to account for a design, budgeting, and implementation cycle. NRG asserts that registered entities would require at least an additional 12 months to train and adapt personnel to procedural changes for a total of three years implementation [similar to a V3 to V5 transition].
Likes 0	
Dislikes 0	

Response
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2
Answer	
Document Name	
Comment
24 months is needed at a minimum. Entities need to reevaluate technologies currently used to manage processes supporting compliance to the requirements. This is particularly important with transitioning from patch management to vulnerability management. This will most likely require capital investments, which require adequate budget time.
Likes 0	
Dislikes 0	
Response
David Jendras - Ameren - Ameren Services - 1,3,6
Answer	
Document Name	
Comment
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)
Likes 0	
Dislikes 0	
Response
Gladys DeLaO - CPS Energy - 1,3,5
Answer	
Document Name	
Comment
2 years (budgetary reasons, training, reconfiguration of systems, compliance with Secure Configuration, risk analysis, etc.)
Likes 0	
Dislikes 0	
Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BHP anticipates it would take eighteen to twenty-four months to implement these changes.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	
Document Name	
Comment	
Tri-State recommends an implementation timeframe of 24 months after approval by FERC. This will give entities time to understand the changes to the standards and then design, test, and implement program changes.	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
Recommend at least 36 months to perform architecture redesign, documentation updates, and documentation reviews. Dial-up is employed at many locations throughout our company and a significant amount of work will need to be completed to meet the requirements in the Standard especially with the removal of ERC, BCA, and ESP from the Standards. In addition, budgets are completed annually so if additional equipment is required it would need to be included in annual budget cycles. Because of the extensive amount of changes currently proposed we recommend a NERC sponsored pilot program similar to what was done for CIP Version 5.	
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 no Dominion and NYPA	
Answer	
Document Name	
Comment	
Three years because this change is similar in scope to upgrading from CIP version 3 to 5. We suggest borrowing from that earlier implementation plan, where each Entity had the option of which version to adhere to and by BES Cyber Asset / BES Cyber System (instead of wholesale conversion).	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	
Document Name	
Comment	

The SSRG suggests 24 months to ensure adequate artchitechture design, documentation updates, and documentation review.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	
Document Name	

Comment
abstain

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
Given that these changes will require Responsible Entities to review internal program documentation and potentially make signification changes to their programs, 36 months is a reasonable timeframe for successful implementation of the necessary changes. The changes required for internal program documentation and coordination of these changes across large enterprises will take time to develop and implement. For Registered entities that choose to shift from an asset-based CIP philosophy to a system-based one, the change of alignment will be a significant program change. Changing configuration management from our current methodology (logical to system or system to logical) will take significant time to change and also what and how we gather the required evidence to demonstrate compliance. Enumerating the change will require new processes. New processes will take time to implement.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	
Document Name	

Comment
PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	
Document Name	

Comment
24 months

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment
At a minimum, APPA recommends that the timeline for the Implementation Plan be 24 months. Public power companies believe Virtualization will be a challenge that will exceed the transition from CIP Version 3 to Version 5. Implementation will require significant time and resources. Consequently, sufficient time and an appropriate compliance approach will be needed to ensure successful implementation. Because of the extensive, untried nature of the changes, we strongly urge a NERC-sponsored pilot program with volunteer entities, analogous to that undertaken for the CIP v5 changes. The implementation timeline might be minimized under a “virtualization overlay” approach, in which entities can elect to stay with existing definitions and requirements or move to the new ones (on a cyber-system by cyber-system basis). Perhaps 12 or 18 months might suffice in such a case, which would allow interested entities to exploit as soon as possible the possibilities of virtualization.

Likes 0	
Dislikes 0	

Response

11. The SDT is proposing conforming modifications to CIP-004. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. Modifications related to CIP Exceptional Circumstances

b. Use of newly proposed terms EACS and EAMS in the Applicable Systems column

c. Addition of PCS to the Applicable System column for Parts in CIP-004 to mitigate security risks associated with individuals not needing authorization or PRAs when granted access to systems inside the Logical Isolation Zone

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	Yes
Document Name	

Comment

SMEC agrees with modifications related to CIP Exceptional Circumstances. SMEC believes further guidance should be provided to define the split of EACMS.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

We are in agreement with the changes related to CIP Exceptional Circumstances, the use of the newly proposed terms EACS and EAMS, and the addition of PCS. However, we believe it would also be prudent to include PCS under CIP-004 R2. Individuals who have access to PCS have access to systems inside the LIZ and should be trained on the security risks accordingly.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	Yes
Document Name	

Comment
We support the changes related to the EACMS and PACS. As we suggested in the above question 6, the LIZ should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	

Comment
No comment.

Likes 0	
Dislikes 0	

Response

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

Comment
a. The modification to CEC is appropriate for CIP-004. b. There are concerns around revocation of access in a timely fashion if a third party service is used for monitoring of EAMS and PAMS. c. The definitions for Protected Cyber Systems and Logical Isolation Zone lose the "routable" distinction for communications. This is somewhat addressed in CIP-005-7 1.2.1, but recomend it remain in the definition. Also, the LIZ definition doesn't define "communications" or "controls," so exactly what will define this zone? A modem can be said to "control communications." The definition of LIZ is too vague.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
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	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 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	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
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	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
Button response should be "No". Button selection wasn't allowed. PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. The SDT did a good job here. PAC disagrees with EACMS and PACS changes and believe we can accomplish the same without the new terms. If the PCS is going to be added to the R3 applicability is should be added consistently to CIP-004 and be added to R2.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

APPA believes the modifications to CIP Exceptional Circumstances (CEC) are appropriate. However, the SDT needs to verify that standards being balloted separately (CIP-008 for example) are considered and included appropriately for CEC. This is especially important for CIP-008 given that the definition of CEC includes language on Cyber Security Incidents.

The only place that EAMS and PAMS appear in the revised standards is under requirement language in CIP-004 R4 and R5. Public power believes that the CIP-004 update does not alleviate third party provider concerns with PAMS and EAMS. See discussion under Question 4.

Public power does not agree with the expansion of applicability for CIP-004 R3, R4, and R5 to include PCS. Changes in these Applicability Systems are not consistent with this Standard's Purpose statement.

If PCAs were not included originally and the SDT is not following a FERC order to do so, then there is no reason to make them applicable. In CIP-004, R4, and R5 the terms EAMS and PAMS are selectively included in the Requirement language.

In general, the necessity to expand the scope of CIP Standards to address new vulnerabilities introduced by virtualization can be minimized or eliminated by use of the dual-definition/parallel requirement "virtualization overlay" approach discussed above.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment

Cowlitz supports APPA comments.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

a. Texas RE agrees with the addition of the CIP Exceptional Circumstance language to proposed CIP-004-7 R3, Part 3.5.

b and c. Please see comments in question #4 related to the applicability of ECMS and EAMS. If the industry wants to revisit the applicability of the requirements to various systems, Texas RE recommends this be done in a separate project where a standard drafting team can perform a holistic review of all CIP standards.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST agrees with modifications related to CIP Exceptional Circumstances and addition of PCS to certain Parts in CIP-004. However, N&ST objects to the proposal to make newly-defined EAMS and PAMS subject only to CIP-004 (as per our response to Question 4).	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Please clarify if EAMS and PAMS are to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if EAMS and PAMS are to be treated similar to BCSI, which appears to be the case. If they are intended to be treated similar to BCSI, they should not be included in the applicable systems column. They should only be in the requirements column. The periodic review requirements need to be clarified based on the intent. As written, you are requiring quarterly review of BCSI-like repositories. You are also requiring two different types of access reviews every 15 months. This seems duplicative and inappropriate. The same issues are present with the access revocation tasks under Requirement R5.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"Although EEI does not agree with the modifications related to CIP-004 as described above, we do support the modifications to the CIP Exceptional Circumstances. Also, we do not support the modifications to the proposed retirement of EACMS, ESP, EAP, etc. for the reasons previously stated in our comments."

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	
Comment	

Although Exelon does not agree with the modifications related to CIP-004 as described above, we do support the modifications to the CIP Exceptional Circumstances. Also, we do not support the modifications to the proposed retirement of EACMS, ESP, EAP, etc. for the reasons previously stated in our comments.

Likes 0	
Dislikes 0	
Response	

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	
Comment	

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 11.

Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	
Comment	

Yes – CIP Exceptional Circumstances

No – EAMS and EACS

Yes – Addition of PCS

Disagree with the use of EAMS and PAMS in the applicable systems column. One significant issue that is being studied is the use of cloud storage and the use of remote monitoring by professional services firms that have higher levels of security skill than many entities. By including EAMS and PAMS in CIP-004 requirement part 4.1, this difficulty is perpetuated.

In its place, Wabash Valley recommends a new CIP-004 requirement part governing for access to EACS, EAMS, PACS, PAMS, governing electronic access, physical access, and BCSI Storage location access to:

Identify and demonstrate that access controls have been implemented by the entity or through implementation of a widely accepted independently audited certification such as ISO 27001, FEDRAMP, <Canadian Equivalent to FEDRAMP> or <Mexican Equivalent to FEDRAMP>.

May need to add an additional part or language to address the case of a withdrawn certification.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does not agree with the majority of the modifications related to CIP-004 as described above, however, NV Energy does support the modifications to the CIP Exceptional Circumstances. Also, we do not support the modifications to the proposed retirement of EACMS, ESP, EAP, etc. for the reasons previously stated in our comments.

NV Energy believes that the revisions to the definitions are unnecessary at this time, and can be addressed through correct identification of PCA within the existing CIP Standards language.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

MISO supports the shift to EACS and EAMS. MISO encourages the SDT to reinforce the differences between the security requirements for the monitoring and the access functions.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	
Comment	
If a device is classified as an EAMS or PAMS, does that require the device to be considered a BES Cyber System Information storage location? What about third-party hosted EAMS/PAMS and the implications to CIP-004 controls?	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
The addition of PCS to CIP-004 increases the documentation burden to entities who will now have to identify additional systems and those who have access. Documentation of access to a BCS and LIZ should suffice and imply access to associated PCS.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
If the stated intent of the creation of EAMS is “to allow third party monitoring systems” and PAMS is “to allow third party monitoring or event correlation”, BPA believes this is not specifically supported in the requirements CIP-004 R4.1/4.2 since CIP-004 R4.2 directs “Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.” If the intent is to allow third part monitoring, there needs to be a way to allow authorization on a vendor or provider basis. BPA suggests this could be done via contract language or grant to that company. This exists in CIP-004 R5.1, 5.2, 5.3 and anywhere else action on an individual basis is required.	
Likes 0	
Dislikes 0	
Response	

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

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project

Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

a. Reclamation agrees with the modifications related to CIP Exceptional Circumstances. CIP Exceptional Circumstances are necessary during emergencies for first responders.

b. Reclamation disagrees with the proposed terms EACS and EAMS in the Applicable Systems column. Reclamation recommends the SDT use Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) instead, as stated in the response to Question 4.

c. Reclamation agrees with the addition of PCS in the Applicable Systems column for CIP-004; however, Reclamation does not agree with the proposed PCS definition. The system wide approach does not allow for the detail needed to properly address all security issues.

Reclamation recommends changing the PCS definition

from:

Cyber systems that can communicate with a BES Cyber System from within the BES Cyber System's Logical Isolation Zone. The impact rating of Protected Cyber Systems is equal to the highest rated BES Cyber System within the Logical Isolation Zone.

to:

One or more Cyber Assets that can communicate with a BES Cyber System from within the BES Cyber System's Electronic Security Enclave. The impact rating of Protected Cyber Systems is equal to the highest rated BES Cyber System within the Electronic Security Enclave.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

Recommend changing from Logical Isolation Zone to Logical Security Zone

Changes in these Applicability Systems are not consistent with this Standard's Purpose statement

Changes to Applicability Systems in 4.2 – 4.5 and 5 increase the workload. This increase will negatively affect focus on BES Cyber Systems with a decrease in cyber security effectiveness

This CIP-004 update does not alleviate third party concerns with PAMS and EAMS. Should CIP-005, CIP-006, CIP-007 and CIP-010 have matching updates.

In CIP-004, R4 and R5 the terms EAMS and PAMS are selectively included in the Requirement language. Request clarification since these systems are already included in the Applicable Systems column.

Request clarification on CIP Exceptional Circumstances because there is some confusion. Some changes are the main Requirement level. Others are at the sub-Requirement level. Expected all these changes at the main Requirement level.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

MEC does agree with some of the modifications related to CIP Exceptional Circumstances, such as adding it back to CIP-004-6 R3, but we do not agree with the conforming changes resulting from the retirement of EACMS, ESP, EAP, etc. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
a. We conceptually agree to the proposed changes for CIP Exceptional Circumstances. b. We conceptually agree to the proposed changes for EACS and EAMS. c. We conceptually agree with the addition of PCS into the access control program in CIP-004 however at the substation level, there may be technical issues in applying the same access controls program to all existing PCS devices. This may require wording “per PCS capability” or similar into some CIP-004 requirements	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
a. Agreed b. Proposed definitions need to be re-evaluated. c. Agreed with the following caveat; that read-only systems that are currently viewed as IRA requiring intermediate systems should be excluded or handled differently.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP does not agree with the expansion of applicability for CIP-004 R3, R4, and R5 to include PCS. If PCAs were not included originally and the SDT is not following a FERC order to do so, then SRP does not see a need to add them to the applicability. SRP also agrees with APPA's comments.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Support MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	

Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company agrees with the CEC additions and with the addition of PCS to the applicability of these requirements. However, we disagree with the inclusion of EAMS and PAMS throughout R4 and R5. Southern asserts that retaining EAMS and PAMS on these requirements prevents the results the SDT has stated as reasons for splitting these terms. Entities will still not be able to utilize vendor or government agency services that can enhance reliability and security and help detect cyber-attack activity early in the kill chain if we shackle the entities with requirements on the personnel or devices/systems at those outside entities. We suggest the SDT consider the need for these terms at all. Can government “cloud service” certification (FedRAMP, etc.) help achieve the same data security end goal when external parties are involved? If the three letter government agencies can certify against a government body (FedRAMP), we assert that we should be able to do the same.	

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

abstain

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 no Dominion and NYPA

Answer	No
Document Name	

Comment

Recommend changing from Logical Isolation Zone to Logical Security Zone

Changes in these Applicability Systems are not consistent with this Standard's Purpose statement

Changes to Applicability Systems in 4.2 – 4.5 and 5 increase the workload. This increase will negatively affect focus on BES Cyber Systems with a decrease in cyber security effectiveness

This CIP-004 update does not alleviate third party concerns with PAMS and EAMS. Should CIP-005, CIP-006, CIP-007 and CIP-010 have matching updates.

In CIP-004, R4 and R5 the terms EAMS and PAMS are selectively included in the Requirement language. Request clarification since these systems are already included in the Applicable Systems column.

Request clarification on CIP Exceptional Circumstances because there is some confusion. Some changes are the main Requirement level. Others are at the sub-Requirement level. Expected all these changes at the main Requirement level.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Tri-State requests rewording of the Requirements R4.1.3 and R4.4 to clarify if it is the the access type or reposity type that is qualified with "physical or electronic." For example, is physical access in scope for electronic repositories?	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
In agreement with BPAs comment - If the stated intent of the creation of EAMS is "to allow third party monitoring systems" and PAMS is "to allow third party monitoring or event correlation", BPA believes this is not specifically supported in the requirements CIP-004 R4.1/4.2 since CIP-004 R4.2 directs "Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records." If the intent is to allow third part monitoring, there needs to be a way to allow authorization on a vendor or provider basis. BPA suggests this could be done via contract language or grant to that company. This exists in CIP-004 R5.1, 5.2, 5.3 and anywhere else action on an individual basis is required.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST.	

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Although the EEI members who participated in the development of these comments do not agree with all of the modifications related to CIP-004 as described above and do not support those modifications to implement the proposed retirement of EACMS, ESP, EAP, etc., EEI does support the proposed modifications to the CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
The exception should be for prior to granting authorized electronic access and authorized unescorted physical access to align with R2.2 training and Part 4.1 process to authorize based on need. Additionlly, if PCS are added to the Applicable System column for Part 3.1–3.5 it should also be included in Part 2.1-2.3. The process to authorize based on need except for CIP Exceptional Circustasnces would also algin.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Please clarify if EAMS and PAMS are to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if EAMS and PAMS are to be treated similar to BCSI, which appears to be the case. If they are intended to be treated similar to BCSI, they should not be included in the applicable systems column. They should only be in the requirements column. The periodic review requirements need to be clarified based on the intent. As written, quarterly review of BCSI-like repositories are required. As are two different types of access reviews every 15 months. This seems duplicative and inappropriate. The same issues are present with the access revocation tasks under Requirement R5.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
The exception should be for prior to granting authorized electronic access and authorized unescorted physical access to align with R2.2 training and Part 4.1 process to authorize based on need. Additionlly, if PCS are added to the Applicable System column for Part 3.1 – 3.5 it should also be included in Part 2.1-2.3. The process to authorize based on need except for CIP Exceptional Circustasnces would also algin.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	

We still have concerns about the splitting of EACMS and PACS into two different types. As mentioned before, has the drafting team considered when a device performs both functions what role it will have? We agree with the modifications related to CIP Exceptional Circumstances. For CIP-004 R5.3, it is unclear why EAMS and PAMS are called out in the requirement when they are also in the applicability column. A BCS by its very nature has BCSI on it. EACMS and PACS (classical definition) may also have BCSI on it. If the SDT still believes that EAM and PAMS need to be called out in the requirement, then we recommend the following modification: “designated storage locations, including EAMS and PAMS, for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end...” Furthermore, CIP-004 R5.3 continues to be broken because technically it only applies to the applicable systems. There is not such concept as a BES Cyber System Information Repository, or storage, either physical or electronic, that contains BES Cyber System Information. All of CIP-011 also only applies to applicable systems. While most companies are applying BCSI protections to those items not listed in the applicable systems, technically they do not have to. However, this appears to be outside the SAR for this effort.

Likes 0	
Dislikes 0	

Response

Nathaniel Clague - Portland General Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

PGE agrees with the changes related to CIP Exceptional Circumstances and PCS, but does not agree with the changes for EAMS and EACS. PGE supports BPA’s comments related to lack of the desired outcome of allowing 3rd parties to perform roles on EACS and EAMS in the proposed applicability tables.

Likes 0	
Dislikes 0	

Response

12. The SDT is proposing modifications to CIP-005 (see the CIP-005 Technical Rationale document for detailed information). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The replacement of the ESP concept with Logical Isolation Zone (LIZ).

b. Is the backward compatibility clear as existing ESPs and EAPs move to the new LIZ concept?

c. The addition of the 4.2.3.3 exemption in the standard along with the addition of Requirement part R1.2 to address the V5TAG concern of "Super ESPs" or single networks within or between BES Cyber Systems that span more than one geographic location.

d. As differing forms of shared infrastructure come into play with virtualization, Requirement R3 has been added to include the management plane and its isolation controls as a part of the CIP standards. Is this concept clearly and widely understood?

Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

I beleive item "a" for LIZ will need more examples to help entities better understand how it can be identified and then documented to help ease any audit concerns.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	

Comment

CIP-005 needs to be renamed. In general, we support the SDTs new definitions and terminology retirements. However, the structure of CIP-005 R1 requires mitigating risk of unauthorized communications, this seems to imply a requirement to authorize communication. Compliance with the new R1 and auditing could be problematic.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	
Comment	
CIP-005 needs to be renamed.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the replacement of the ESP concept with Logical Isolation Zone (LIZ). SRP does not agree the modifications are backwards compatible due to the expansion of applicability for various requirements. SRP agrees with the addition of 4.2.3.3 and the addition of R1.2 to clarify Cyber System geographic spans. SRP would like to see geographic spans more clearly defined as this may imply encryption between our primary and backup control centers. SRP also agrees with the comments from APPA.	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
The concept is clear but is not widely understood. A learning curve is to be expected.	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The concept is understood by people famiar with computing concepts.	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Requirement part R1.2 appears to imply end-to-end encryption as the security objective. We recommend further clarification between CIP-005 R1.2 and CIP-012 to solidify the intent.	
Likes 0	
Dislikes 0	
Response	

Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP recommends the diagrams from the webinar be included in the technical rationale to more clearly illustrate how the concepts of Logical Isolation Zones would be applied to new and virtualization technology.	
Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Regarding c: Encryption should be in place between the two end-points shown in the diagram. Also, the same level of firewall controls should be enabled within both environments. However, there really doesn't seem to be a logical alternative to encryption to allow for disparate LIZs. Regarding d: The management planes should reside in completely isolated layer 3 networks that are not accessible by other workloads or layer stacks from the other LIZs and/or mixed mode environments. VLANS and VXLANS should not be used to isolate the management planes. Additionally, multi-factor authentication should be used along with separate authentication domains. These management planes, if compromised, would provide the “keys to the kingdom.”	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Backwards compatibility seems to be there, but it will require a review of all current network diagrams to see if all of our ESPs can be LIZs or if we want to consolidate/regroup certain systems into a LIZ. R1.2 addresses the fact that LIZ can be in different geographical locations. R3 is not clearly understood.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	

Backwards compatibility seems to be there, but it will require a review of all current network diagrams to see if all of our ESPs can be LIZs or if we want to consolidate/regroup certain systems into a LIZ. R1.2 addresses the fact that LIZ can be in different geographical locations. R3 is not clearly understood.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
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	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	

Comment
Button response should be "No". Button selection wasn't allowed. PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. The SDT did a good job here. {C}a) Comments above in #6 cover the LIZ {C}b) Yes {C}c) PAC appreciates the exception language related to the implementation of the super ESP. {C}d) In CIP-005-7 the SDT capitalized the two terms Management Plane and Data Plane. Was this intentional? PAC understands the concepts presented.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment
a. Texas RE does not agree the ESP concept should be replaced with Logical Isolation Zone (LIZ), since LIZ currently can exist within the current ESP concept. Please see Texas RE's response to #6. b. Registered Entities may or may not be "backward compatible" with the LIZ concept. The LIZ concept would require network zoning, where ESP concept currently does not. If registered entities do not having network zoning, they would not be backward compatible. Texas RE notes that the LIZ concept can currently be done within the ESP concept. c. Texas RE maintains ESP and EAP do nit need to change, so the exemption in CIP-005 Part 4.2.3.3 exemption is not needed. Texas RE agrees with CIP-005 Part 1.2 but it should say "Protect the data traversing communication networks used to provide connectivity between **ESPs** that spans multiple geographic locations to preserve confidentiality and integrity."

c. Texas RE agrees with CIP-005 Part 3.1 and acknowledges that it does address virtualization. Texas RE recommends the following in the Applicable Systems column:

- EACS and PCS should be replaced with EACMS and PCA
- There appears to be a typo: "*Medium Impact BES Cyber Systems and their associated **PCS***"; "PCS" should be removed.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment

Cowlitz agrees with APPA comment.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3

Answer	
Document Name	

Comment

While Virtualization needs to be addressed, additional implementation guidance is needed on "how" to treat virtualization, especially the isolation of BES vs. non-BES Cyber Assets on the same virtual infrastructure. Most entities have been separating the two; however, this separation is more costly.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	

The virtualization changes that are proposed will likely permit some mixed trust applications but it isn't yet clear how logical isolation zones will provide better or equivalent protections to that of an ESP.

12.c. MRO supports the concept of a "Super ESP" that leverages encryption or equivalent logical protections initiated and terminated inside geographically separated ESP locations. The Logical Isolation Zone described in the 4.2.3.3 exemption however is not yet understood to be an equivalent or superior security protection.

Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

a. APPA agrees with the replacement of the ESP concept with Logical Isolation Zone (LIZ). Still better might be the overlay approach, in which both ESP and LIZ are options for an entity. Under such an option the existing definitions of EACMS and ERC might need to be updated to include "…Electronic Security Perimeter or Local Isolation Zone…" (i.e., add LIZ concept) to allow appropriate flexibility.

b. No. See discussion under Question 6.

c. Unclear. There is also concern that new approach to "Super-ESPs" is not backwards compatible as regards to communications among serially-connected BCS without ERC, and for relay tele-protection systems. For serial connected BCS, the new approach appears to expand the scope and treat communications for these cases the same as if there was ERC, which is not the way such cases are audited now. At present, a communication "demarcation" is identified for the non-ERC BCS at each end, and communications outside this demarcation are exempted, and no encryption or other security is required. For relay tele-protection, it appears to extend the BCS to include both ends, thereby raising to Medium any otherwise Low-impact rated substation connected by tele-protection to a Medium rated substation. Again, this expands the scope. In general, as a guiding principle, any expansion of scope to accommodate new vulnerabilities introduced by virtualization should be limited in applicability only to virtualized BCS.

d. Public power generally agrees with the addition of 4.3.3.3 and the addition of R1.2 to clarify Cyber System geographic spans. However, these additions do have several aspects that raise questions. For example, Requirement R3 regarding management plane concept will require implementation to understand the implications. Will there be a need to "future proof" the language related to the R1 exclusion? How will registered entities document the exclusion of time-sensitive protection or control functions?

Likes 0	
Dislikes 0	
Response	

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

a. Agree, although it creates a documentation burden.

b. Yes

c. How are entities to document exemptions?

d. How will the removal of the term ERC affect serially connected substations where no remote access capability exists?

Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

(a) LIZ may be better understood once additional clarity on logical security zone is provided. (b) Backward compatability is dependent upon previous questions asked and their results. (c) Yes (d) We believe there are too many dependencies at this stage to determine “clear and understood” status.

CIP-005-7 R1.2: Duke Energy requests clarification on the differences between, or how R1.2 interrelates with CIP-006-7 R1.10. On its face, these two appear to be redundant. Additional language distinguishing one from the other, or perhaps Implementation Guidance on these would be helpful.

CIP-005-7 R3: Is it the SDT’s intent for proposed R3 to be more expansive than what is currently protected? Is the SDT intending to bring in for example, the management interface of a firewall for the EACS?

Likes 0	
Dislikes 0	
Response	

Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	

MISO requests that the SDT:

Unify the terminology between LIZ and "Super-ESP"

Provide clarity on the encrypted/protected data requirement. In particular does this requirement only apply if the data is leaving a PSP and is out in public spaces between the separate parts of the "Super-ESP?" If the requirement applies even when the data is still within a PSP that may require significant network complexity for minimal risk avoidance.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

While we do not have specific comments on questions a-b, we do have a comment on questions c and d and some concerns about certain updates within CIP-005.

c. We would like for the SDT to provide some examples within IG of how ESP would meet the definition of LIZ. We do have some concerns that auditors will need to have additional training to be able to audit the new LIZ.

d. We agree that in a mixed-mode virtual environment, isolation between the management plane and data plane becomes imperative (with mixed-mode meaning, for example, high/medium BES Cyber Systems, BES Cyber Systems/EACS, or CIP/non-CIP). However, if an entity sets up separate virtual environments (i.e. a high impact BES Cyber System virtual environment and a separate associated High Impact EACS environment) we believe that isolation between the management plane and the data plane will require a significant amount of extra work that will result in elevated compliance risk and zero benefit. The SDT should continue to consider that not all virtual environments that involve CIP will be mixed-mode. It should be clear in the requirements that if you protect the management plane as a part of the BES Cyber Systems the isloations requirements of Part 3.1 become nothing more than an exercise for compliance.

Other Comments:

Part 1.4 lists PCS as an applicable system and refers back to groupings under 1.1. However, Part 1.1 does not include PCS. Was this intentional by the SDT? To be consistent, we believe that PCS need to be added to 1.1 or removed from 1.4.

Additionally, the Secure Configuration concept is found throughout CIP-005. Please see our comment relating to Secure Configuration under question 15.

Finally, can the SDT provide information on the difference between CIP-005 R1.2 and CIP-006 R1.10? Under CIP-006 you can use physical protections and/or encryption to protect data that runs between LIZ, this seems to be duplicated under the new requirement of CIP-005 R1.2. We realize that CIP-005 talks about protecting data and CIP-006 discusses the physical protection of the cable, but both requirements are completeing basically the same function. This could result in double jeapory.

Likes 0	

Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment
NV Energy does not support all the changes being considered by the SDT for CIP-005 because we do not agree that the CIP Standards should be upended in order to accommodate a very small number of virtualized systems currently operated or being considered. NV Energy does support the revisions to R1.2 for a “Super ESP”. As an Entity that currently deploys this type of ESP, the inclusion of defining this ESP would improve the existing Auditing practices for this type of system. NV Energy also asks the SDT to consider the broad impacts and risk that the proposed wholescale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While we do not dispute that over time “zone” type security will replace the current “perimeter” type solutions, we disagree that this is the right time for such broad and sweeping changes. Instead, the SDT should take a less aggressive posture toward virtualization and narrow this effort to less complicated steps that might assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky steps that will also reduce security and compliance issues for the industry. Additionally, while the SDT proceeds with this effort, we respectfully ask them to consider providing more time for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	

Comment
CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following: Do the proposed changes intend to include the EACS inside or outside the LIZ? The concept of LIZ is not perimeter based and so it is not clear what or where an EACS is. Previous language was more clear that it was an Access Point, Intermediate System, or internal authentication system (e.g. LDAP inside the ESP).

In the proposed EACS concept, does a host-based firewall count as an EACS? Does a switch with an ACL count as an EACS? Does a network firewall inside an ESP implementing segmentation count as an EACS? Does a system's authorized users and authentication config count as its own EACS? Entities may define, in compliance with CIP-005-7 RequirementR1.1, their EACS protecting their BCS. However, there is compliance risk with the entities' choices because EACS is not well defined as being external to BCS/PCS in the LIZ or at the LIZ perimeter.

Additionally, access to a system using serial connection is allowed in CIP-005-7 Requirement R1.1, but not addressed much elsewhere. Is the intent that requirements for user restriction on IRA, encryption of connection to an intermediate system, and multi-factor authentication at an intermediate system apply to serial connections? This is unclear in the proposed standard.

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	No
Document Name	

Comment

CHPD is concerned about the overlap of CIP-005 R1 Part 1.2 and CIP-006 R1 Part 1.10. The protection of so-called "Super ESPs" seems to already be covered by the CIP-006 R1 Part 1.10. Only one of the requirements should be maintained, and given that CIP-006 R1 Part 1.10 is already in effect, it is CHPD's preference that it be maintained over CIP-005 R1 Part 1.2.

CHPD also has concerns about the ambiguity of the management plane. Many devices do not have dedicated management planes, such as a server with remote desktop enabled. While it is best practice to separate your management plane from your data plane, many devices either would not support that or their function would be greatly degraded by having to disable management capability that cannot be isolated. Additionally, this requirement would apply to EACS, bringing network connectivity requirements to a classification of assets that did not before have connectivity requirements.

The concept of the LIZ does not seem to work if CIP-005 R3 is not considered. Depending on the interpretation of what a management plane is, significant rework of the network may be needed to separate it from the data plane. Take, for example, a PC-based system that is managed using remote management software (RDP, SSH, VNC, etc…). These systems and protocols could easily be considered to be "management plane" without any specific definition or language to say otherwise. The problem with this is that there is no feasible method for separating these kinds of PC-based management services from the "data plane" like can be easily done for a switch, firewall or hypervisor. The current scope of R3 includes BCA, EACS and PCS, so Windows and other similar PC-based Cyber Assets would definitely fall under the requirement, as written. Without a definition for "management plane" that properly scopes devices that do support separation of a management plane (e.g., switches, firewalls, routers, hypervisors, etc…) there is little likelihood that any existing Medium of High Impact-owning entity could establish a method for achieving compliance with this language. One recommendation for fixing this problem is to specifically identify those system types, either by definition or within R3 itself, that require management plane separation.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	
Comment	

Introduction of a new term logical isolation zone rather than ESP introduces confusion in the definition and with backward compatibility. For example, the definition would now be applicable to serial communications. This is an example of a definition that will be debated for several years in the industry. Continue with our current industry standard definition or ESP and adjust the standards language to address issues or adopt standard NIST terms. SuperESPs can be accommodated by changes to requirements rather than definitions as the current definition of an ESP does not prevent multi-site ESPs.

Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 12.

Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	

Exelon does not support the changes being considered by the SDT for CIP-005 because we do not agree that the CIP Standards should undergo this level of significant change for the purpose of accommodating the needs of a relatively small number of mixed virtual environments currently operated or being considered. The proposed change to move from a layer 3 "perimeter" to a "logical isolation zone" philosophy introduces a significant learning curve. There may be serious risks to security through misunderstandings of vulnerabilities and how to properly implement, by both Responsible Entities and auditors.

Exelon also asks the SDT to consider the broad impacts and risk that the proposed wholescale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While we do not dispute that over time "zone" type security will replace the current "perimeter" type solutions, we disagree that this is the right time for such broad and sweeping changes. Instead, the SDT should take a less aggressive posture toward virtualization and narrow this effort to less complicated steps

that might assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky steps that will also reduce security and compliance issues for the industry.

Additionally, while the SDT proceeds with this effort, we respectfully ask them to consider providing more time during the standard development process for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"EEI does not support the changes being considered by the SDT for CIP-005 because we do not agree that the CIP Standards should be upended in order to accommodate a very small number of virtualized systems currently operated or being considered. Additionally, changes such as moving from a “perimeter” to a “zone” philosophy may result in serious risks to security through misunderstandings of what exactly that means by both Responsible Entities and auditors, which is not currently justified.

EEI also asks the SDT to consider the broad impacts and risk that the proposed wholescale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While we do not dispute that over time “zone” type security will replace the current “perimeter” type solutions, we disagree that this is the right time for such broad and sweeping changes. Instead, the SDT should take a less aggressive posture toward virtualization and narrow this effort to less complicated steps that might assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky steps that will also reduce security and compliance issues for the industry.

Additionally, while the SDT proceeds with this effort, we respectfully ask them to consider providing more time for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems."

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

The note should not be used within requirement language in Part 1.1 and other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.

Geographic location should be clarified on Part 1.2. It is unclear how this would apply to multiple buildings within a single campus. These buildings may have different PSPs while in the same campus.

For Part 1.4, consider using “per system capability” instead of “excluding serial port connectivity such as RS-232 and RS-485”.

For Part 2.2, consider the following, “Have one or more methods at the point of termination to mitigate the risks posed by unauthorized modification and unauthorized disclosure of data during all Interactive Remote Access sessions.”

For Part 2.3 consider the following, “Have one or more methods of multi-factor authentication for all Interactive Remote Access sessions.”

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Although N&ST is supportive of the general concept of replacing the network-centric definition of “ESP” with a more flexible, “secure enclave” concept, we have a number of concerns:

>> N&ST believes the current proposed definition of “LIZ” needs to be clarified. Suggested re-wording: “A logical container, or enclave, that encloses one or more BES Cyber Systems and applies a common set of controls to all communications to or from those BES Cyber Systems.”

>> N&ST believes the desired “backward compatibility” needs to be made more clear. N&ST suggestions include (1) revising the definition of “LIZ,” as per above, (2) adding explicit language to R1 to the effect that applicable systems must be located with a “LIZ,” and (3) Cyber Asset(s) used to provide the necessary control of communications into and out of a “LIZ” must, if not already part of an applicable system, be identified as EACMS or EACS.

>> N&ST opposes the proposal to exempt Cyber Assets within a “LIZ” if they are associated with communications links between multiple geographic locations. N&ST believes such an exemption carries the risk of creating “soft spots” within logical boundaries that are supposed to be highly secure.

>> N&ST believes the concept of isolating the management and data planes of virtual systems is reasonably well understood, but we are concerned about the fact there are no further requirement statements about the management plane in any of the modified Standards. N&ST believes that at a minimum, the management plane(s) of virtual systems (e.g., Hypervisor) should be categorized as EACMS or EACS.

>> N&ST has an additional concern about the proposed changes to CIP-005: As written, R1 could, N&ST believes, be interpreted as applying to ALL high and medium impact BES Cyber Systems, regardless of whether or not they communicate using routable protocols.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC disagrees with ESP replacement. It will require additional documentation, especially for serial connected devices. LIZ should only apply to the virtual devices.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

In addition, how is the proposed CIP-005 R1.2 different from CIP-006 R1.10? Seems there is overlap as it relates to encryption of data.

Also, SDT needs to explain the comment “Examples include physical protections and points where encryption initiates and terminates.” Is this suggesting physical protection must be applied to encryption points, or that this requiring both physical measures and encryption?

Need to better define communication networks. Which protocols are in scope vs. out of scope, and how are third-party networks treated?

Regarding CIP-005 R1.4, SDT needs to provide guidance / clarity on the term “privileged introspection.”

And generally speaking, needs to clarify the use of system or asset throughout the standards, as the current proposed revisions do not seem to be consistent, and using undefined terms will make it difficult to establish device applicability.

Regarding the Virtual Machine concept, the entire Virtual Machine / system, including the hypervisor, must be part of the BCS with CIP controls applied. If someone can comprise the hypervisor and disable or compromise the virtual machines / systems (BCS) that could have 15-minute impact, it should also be a BCS. High-water mark everything or require segmentation.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO

Answer	No
Document Name	

Comment

Please see MRO NERC Standards Review Forum (NSRF) comments.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5

Answer	No
Document Name	

Comment

PSE supports the comments developed by EEI.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	
Support MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
As stated in #6 LCRA has concerns about the implementation of the LIZ definition in its current form.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
a. Agreed with the following caveat; the proposed definition of LIZ needs to be re-evaluated and clarified. b., c., d. The proposed definitions need to be re-evaluated and clarified before additional meaning full comments can be considered.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No

Document Name	

Comment

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

- No. We do not think ESP needs to be changed.

  No. We think it will require additional documentation, especially for serial connected devices.

  Yes.

No. We question how this applies to technology such as the Dell DRAC or large network backplane systems.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	AZPS Comments - Question 12.docx

Comment

Please see the attached document.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

a. Agree

b. Agree

c. Agree

d. We understand the concept of isolation between the management plane and the data plane, however there was no discussion or explanation of the CIP controls that may be required for the management plane (aka Central Management Servers ?)

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

More education is needed before implementing such changes. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

Changing from ESP to LIZ is unclear and requires a change in the fundamental understanding to the cyber security that is in place today

Also a scope change because Medium Impact had two variations. For certain Requirements, BES Cyber Assets had exceptions when there was no External Routable Connectivity

Part D we do not believe that the concept of isolated and control of the management plane is widely understood.

We do not support the changes being considered by the SDT for CIP-005 because we do not agree that the CIP Standards should be upended in order to accommodate a very small number of virtualized systems currently operated or being considered. Additionally, changes such as moving from a “perimeter” to a “zone” philosophy may result in serious risks to security through misunderstandings of what exactly that means by both Responsible Entities and auditors, which is not currently justified.

We also ask the SDT to consider the broad impacts and risk that the proposed wholescale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While we do not dispute that over time “zone” type security will replace the current “perimeter” type solutions, we disagree that this is the right time for such broad and sweeping changes. Instead, the SDT should take a less aggressive posture toward virtualization and narrow this effort to less complicated steps that might assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky steps that will also reduce security and compliance issues for the industry.

Additionally, while the SDT proceeds with this effort, we respectfully ask them to consider providing more time for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC

Answer	No
Document Name	

Comment

It appears that the intent of modification to CIP-005 R1.1 was to shift from an isolated ESP to an isolated LIZ. However, as drafted, it appears that this modification either (a) raises the burden by requiring firewalls on every BCS, or (b) uses the “system or group” term to refer to an LIZ. The language “applicable systems, either individually or as a group,” should be replaced with the term “LIZ.” The term “communication” could be augmented with “and access to internals and shared resources,” which would imply not only routable communication but also other mechanisms that could affect an LIZ.

The proposed CIP-005 R1.2 may be redundant with CIP-006 R1.10.

CIP-005 R3 needs additional clarification under “Applicable Systems” in order to be backward-compatible. It may need a new class of asset such as “Zone Boundary System” to apply to. The intent of the Requirement appears to be to prevent an attacker from breaking LIZ boundaries. Most BCS, when they do have a management plane, do not have a management plane that can be used to break an LIZ boundary. If all aspects of a BCS, including management plane and internal virtualized Cyber Assets, are contained entirely within the same LIZ, then no change to its topology can break out of the LIZ. Only an asset that contains some part of an LIZ, but that has some presence in a zone external to the LIZ, could be used to gain unauthorized entry. That would be a Zone Boundary System. An example would be a hypervisor that contains a virtual switch with BCS on it. Access to the management plane of a Zone Boundary System could be used maliciously to reconfigure the virtual isolation and connect those BCS to external systems. Therefore, the proposed R3.1 should apply to Zone Boundary Systems associated with a Medium-Impact LIZ. The management plane should be considered a PCA at the “high water mark” rating of the LIZs contained within and should itself be entirely contained within a LIZ.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

a. No. Reclamation does not support replacing ESP with Logical Isolation Zone (LIZ) as stated in the response to question 6. Reclamation recommends the SDT use the term Enclave to meet FERC's intent.

If new terminology is needed, Reclamation recommends using existing definitions from the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298), specifically the NIST-defined terms "Enclave" and "Enclave Boundary."

Reclamation also recommends replacing the proposed Logical Isolation Zone (LIZ) term with the following term and adding it to the NERC Glossary of Terms:

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

b. No. Reclamation does not support the term LIZ and recommends the SDT adopt the term ESE as described above and in the response to question 6. The proposed LIZ definition seems to combine the ESP and EAP concepts but is not as well defined as the individual ESP and EAP definitions.

Logical isolation must distinguish between BES and non-BES. A Logical Isolation Zone could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on common hardware between CIP Applicable Systems and corporate business networks could introduce risk to the BES.

c. No. As it is written, exemption 4.2.3.3 does not distinguish between entity-owned Cyber Assets and third party-owned Cyber Assets. Reclamation recommends the SDT clearly state the scope of the exemption.

Reclamation also recommends that Cyber Assets associated with communication networks and data communication links used to extend an Electronic Security Enclave to more than one geographic location be protected.

d. No. Requirement R3 seems to apply to Virtual Machines, but it is unclear what the "management plane" and "data plane" are relative to the Applicable Systems. Reclamation recommends the SDT align Requirement R3 to be backwards compatible with current configurations, or state that R3 specifically applies to Virtual Machine technology. Reclamation also recommends if the SDT does use the terms "Management Plane" and "Data Plane" in the standard, they should be defined in the NERC Glossary of Terms.

Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	

We disagree with these changes. For the bullet a & b, we have the same comments as the above question 6. For the bullet c, the communication components between ESP at Control Centres has been addressed in CIP-006-6 R1.10, if SDT wants to protect the communication components between ESPs outside the Control Centres, SDT only needs to develop an additional requirement in CIP-006-6 to address that. For the bullet d, given that the current CIP V5 requirements have addressed the management plane implicitly, where the management plane devices must have been identified as EACMS since they can add, delete or modify CIP VMs and entire infrastructures. In our virtual environment, the management plane devices were identified as Intermediate Systems and fully compliant by the existing requirements.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

We do not think ESP needs to be changed.

a. No. The NSRF believes ESP replacement will require additional documentation, especially for serial connected devices.

b. No. The NSRF does not recommend replacing ESP with Logical Isolation Zone (LIZ).

c. No. The NSRF questions how this applies to technology such as the Dell DRAC or large network backplane systems.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro agrees with the changes outlined under points 12a, 12b and 12c. However, on Question 12d additional clarification is needed, as it seems unclear what aspects of a system, and its functions and types of access (e.g. system to system or user remote access) would be considered part of the management or the data plane in both virtual and physical environments.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

The replacement of ESP to LIZ is appealing, but its ramifications have yet to be fully understood. While an existing ESP/EAP model may be able to port to the LIZ, the problem is the drafted changes have introduced other LIZ that may need to be implemented to be compliant with regard to serial communications and management planes. Per previous comments, we are still concerned about the issue of nesting LIZ and Entities being penalized for defense in depth when a single control fails, yet all other controls were still protecting the applicable systems.

The concept of “span more than one geographic location” gives us pause. The issue is what defines a geographic location. Per https://sciencing.com/geographic-location-mean-8667.html, a “Geographic location refers to a position on the Earth. Your absolute geographic location is defined by two coordinates, longitude and latitude.” The issue is what is the difference in longitude and latitude that constitute one geographic location be separate from another? Longitude can vary depending on the latitude that it is measured at. So just looking at latitude, one degree of latitude can span about 69 miles, a minute of latitude can span about 1.15 mi, and a second of latitude can span about 101 feet. So technically if you have a big enough campus with an A and B datacenter at the campus then you could have a network spanning more than one geographic location when measured down to the second of latitude and longitude. We applaud the SDT for actually trying to tackle a V5TAG issue since this has not been done for the issues of “Clarify the intent of ‘programmable’ in Cyber Asset”, “Clarify and focus the definition of ‘BES Cyber Asset’” and its three sub concerns, the issue of "associated" in the ERC definition, the concept of “directly” within the ERC definition, and the issue of IRA definition with “using a routable protocol” and the Guidelines and Technical Basis contradiction of dial-up connectivity for IRA means that R2 also applies. These are all the items in the SAR not addressed by the SDT in this proposed draft.

The concept of requiring a LIZ for the management plane is not clearly understood. Some devices may inherently come with a separate management plane interface like baseboard management controller on a server (e.g. HP iLO, DELL iDRAC, Cisco CIMC). However, many do not. Servers acting as a hypervisor have Network Interface Cards (NIC) assigned to various functions. Best practice would have a split of the data plane, management plane, storage plane, and motion or migration plane. However, the data plane and management plane can be on the same set of NICs and separated by VLANs. Since this separation is a design choice and not an inherent property, then does that mean all other machines including workstations must be outfitted with a set of management plan NICs per device capability and thus dual-homing all machines to both the management and data plan? While we appreciate the SDT trying to avoid overly prescriptive requirements, the current draft regarding data plane and management plane remains vague and open to varying interpretations of what compliance looks like.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
NRG does not agree with the replacement of the ESP concept with Logical Isolation Zone (LIZ) because serial ports and potentially 4-20mA inputs would be included under EAC or EAPs. Therefore, it would be difficult for registered entities' NERC CIP subject matter experts to understand and potentially difficult to implement as it would take significant resources for registered entities to revamp their entire NERC CIP compliance programs to accommodate these changes, which could affect their existing reliability or security postures. These proposed changes include fundamental changes to NERC CIP ESP and BCS concepts. No, NRG does not assert that backward compatibility is clear as existing ESPs and EAPs move to the new LIZ concept, because it is not technically explicit and not explicit in its technical definition (no clear logical boundaries "in or out" due to retired key terms that help to build the framework of an ESP boundary). This could cause reduced security and less ability to achieve compliance because it requires registered entities to take a more interpretive stance on achieving compliance as the proposed language is less prescriptive. No, NRG does not agree that the addition of the 4.2.3.3 exemption in the standard along with the addition of Requirement part R1.2 to address the V5TAG concern of "Super ESPs" or single networks within or between BES Cyber Systems that span more than one geographic location, because NRG takes the 4.2.3.3 exemption to relate to VLANS. Attackers could manipulate network gear in-between EACs to compromise VLAN security. No, NRG does not agree that as differing forms of shared infrastructure come into play with virtualization, Requirement R3 has been added to include the management plane and its isolation controls as a part of the CIP standards concept is clearly and widely understood. Registered entities would likely need to form additional understanding of these concepts with their vendors which may be broader than the intent of the proposed standard change.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The note should not be used within requirement language in Part 1.1, or in other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location. Geographic location should be clarified on Part 1.2. It is unclear how this would apply to multiple buildings within a single campus. These buildings may have different PSPs while in the same campus. For Part 1.4, consider using "per system capability" instead of "excluding serial port connectivity such as RS-232 and RS-485." For Part 2.2, consider the following, "Have one or more methods at the point of termination to mitigate the risks posed by unauthorized modification and unauthorized disclosure of data during all Interactive Remote Access sessions." For Part 2.3 consider the following, "Have one or more methods of multi-factor authentication for all Interactive Remote Access sessions."	
Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The EEI members who participated in the development of these comments do not support the changes being considered by the SDT for CIP-005 because they do not agree that the CIP Standards should be upended in order to accommodate a small number of virtualized systems currently operated or being considered. Additionally, there is concern that changes such as moving from a “perimeter” to a “zone” philosophy may introduce security risk due to misunderstandings or disagreement on these terms by both Responsible Entities and auditors. EEI recommends that the SDT consider the broad impacts and risks that the proposed wholesale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While there is no dispute that, over time, “zone” type security may replace the current “perimeter” type solutions, now may not be the right time for such broad and sweeping changes. Instead, we recommend that the SDT consider a less aggressive posture and narrow this effort to focus on targeted efforts to assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky actions toward virtualization that will reduce the potential for security and compliance issues as the industry matures toward virtualized systems. Additionally, as the SDT proceeds with this effort, EEI respectfully requests that they consider providing more time for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
a: The concept of the LIZ allows for the introduction of new technologies to fulfill the requirements which is good. However, with a wide variety of possible solutions to available to fulfill the requirements there could also be a wide variety of audit approaches/auditor preferences that could make audits more challenging. b: Yes, a traditional ESP/EAP design seems to fit into the LIZ concept as is. c: No issues with the 4.2.3.3 exemption or the “Super ESP” concept. d: No issues with requirement R3 either, it’s logical and prudent.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
For clarity, Tri-State recommends Part 1.1 R1.1.1 be changed from "and" to "or" to accommodate different configurations and allow flexibility. This should read "Communication that has documented inbound and outbound access permissions, including the reason for granting access; or" Serial port connectivity….	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

a. We do not agree with replacing the ESP concept with LIZ. Is it the intent of the SDT that existing ESPs simply convert to a LIZ, where virtual technology does not exist?

b. With all the additions, deletions, and revisions to so many terms and definitions it is not possible at this time to be sure of backwards compatibility.

c. Unclear

d. Also, in R3 Isolation of Management Plane and Data Plane, these terms are initially defined in footnotes, and then capitalized in M3, then lower case again in 3.1. These terms should be explicitly defined in the Glossary.

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 no Dominion and NYPA

Answer	No
Document Name	

Comment

Changing from ESP to LIZ is unclear and requires a change in the fundamental understanding to the cyber security that is in place today

Also a scope change because Medium Impact had two variations. For certain Requirements, BES Cyber Assets had exceptions when there was no External Routable Connectivity

Part D we do not believe that the concept of isolated and control of the management plane is widely understood.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Southern supports the direction of CIP-005 and logical isolation of systems. We have concerns regarding R3 as it applies to all high and medium impact systems and not just those that utilize shared infrastructure. It is not clear exactly what the management plane and the data plane is on every high or medium impact system in existence. The data plane for instance is defined as "part of the network that carries user traffic" per the footnote. It is not clear how an entity on a firmware-based system with one network port will isolate the management plane from "the part of the network that carries user traffic." We also believe R1.2 is not scoped correctly. The language scopes it to all data on any network (LAN or WAN) within the "components of a LIZ" if that LIZ happens to span geographic locations. It needs to be scoped to just those networks used to span the different geographic locations and not all components within the LIZ, such as two hosts in the same cabinet. For R1, Southern is concerned over the "Secure Configuration" and its

interaction with a "method" of isolation and change management in CIP-010. Devices such as LAN/RAN serial converters and Dynastars (i.e. mixed serial and IP configurations) and how to implement them need additional clarity. If a particular device cannot support encryption but the rest of the devices can, will I be able to reasonably scope my secure configuration at the device level for components, but also have a separate secure configuration for the “rest of the system”? R3 does not fit non-virtualized environments well.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

a. No. WAPA does not support replacing ESP with Logical Isolation Zone (LIZ) as stated in the response to question 6. WAPA strongly recommends the SDT use the term Enclave to meet FERC’s intent.

WAPA recommends using existing definitions from the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298), specifically the NIST-defined terms “Enclave” and “Enclave Boundary.”

WAPA also recommends replacing the proposed Logical Isolation Zone (LIZ) term with the following term and adding it to the NERC Glossary of Terms:

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

b. No. WAPA does not support the term LIZ and recommends the SDT adopt the term ESE as described above and in the response to question 6. The proposed LIZ definition seems to combine the ESP and EAP concepts but is not as well defined as the individual ESP and EAP definitions.

Logical isolation must distinguish between BES and non-BES. A Logical Isolation Zone could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on common hardware between CIP Applicable Systems and corporate business networks could introduce risk to the BES.

c. No. As it is written, exemption 4.2.3.3 does not distinguish between entity-owned Cyber Assets and third party-owned Cyber Assets. WAPA recommends the SDT clearly state the scope of the exemption.

WAPA also recommends that Cyber Assets associated with communication networks and data communication links used to extend an Electronic Security Enclave to more than one geographic location be protected.

No. Requirement R3 seems to apply to Virtual Machines, but it is unclear what the “management plane” and “data plane” are relative to the Applicable Systems. WAPA recommends the SDT align Requirement R3 to be backwards compatible with current configurations, or state that R3 specifically applies to Virtual Machine technology. WAPA also recommends if the SDT does use the terms “Management Plane” and “Data Plane” in the standard, they should be defined in the NERC Glossary of Terms..

Likes 0	
Dislikes 0	

Response

13. The SDT is proposing conforming modifications to CIP-006. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. Modifications related to CIP Exceptional Circumstances

b. Use of newly proposed term EACS in the Applicable Systems column

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
SMEC agrees with modifications related to CIP Exceptional Circumstances. SMEC believes further guidance should be provided to define the split of EACMS	
Likes 0	
Dislikes 0	
Response	

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
b. The SDT has correctly identified that EACS and EAMS should not require the same CIP protections.	
Likes 0	
Dislikes 0	
Response	

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

Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment
If a system that controls access to a BES Cyber System (EACS) is compromised, the real-time ability to operate or control the BPS could be reduced or severed altogether. For this reason, we are in agreement with the use of the newly proposed term EACS throughout CIP-006. Additionally, the modifications related to CIP Exceptional Circumstances bring continuity throughout. See comment in question 12 about CIP-006 R1.10.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	Yes
Document Name	

Comment
We support the changes related to the EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment
Recommend removing TFE from CIP-006 Part 1.3 similar to the removal of TFE from CIP-007.

Recommend having a process to define a PACS asset, including required Identification and classification.

Recommend requiring a response process for the 15 min alarm.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

Add CIP Exceptional Certcumstances for CIP 006 R1.3 to allow for emergency personell to respond without a requirement of two factor authentication

Likes 0	
Dislikes 0	

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC

Answer	Yes
Document Name	

Comment

These changes appear reasonable. Changes to CIP Exceptional Circumstances relieve controls on authorized persons but remove such relief for visitors during CIP Exceptional Circumstances. Relieving controls on authorized persons is consistent with the concept that authorized people may need to act outside of the normal controls. However, authorizing or controlling visitors remains important. Corresponding reliefs under CIP-004 make it possible to grant new authorizations without the lead time of a PRA process, allowing (but still requiring) rational management of emergency staff augments such as incident management consultants during CIP Exceptional Circumstances.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	
Comment	
a) no comment b) no comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the update to include EACS in place of EACMS. SRP also agrees with adding the CIP Exceptional Circumstance exception to the requirements. Additionally, SRP agrees with the comments from APPA.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	

Answer	Yes
Document Name	
Comment	
Hydro One supports TFIST comments suggesting that PACS and PAMS should be subject to maintenance and testing per CIP-006, R3.1.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
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	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
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	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	

Button response should be "No". Button selection wasn't allowed.

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

The SDT did a good job here. PAC disagrees with EACMS and PACS changes and believe we can accomplish the same without the new terms.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

a. Public power agrees with the addition of the CIP to the requirement level for R2. It seems appropriate to maintain the CIP Exceptional Circumstances (CEC) for R1 related to access logs. However, we suggest NERC consider that alarm requirements in R1 could also be covered by CEC in the event of "an imminent or existing hardware, software, or equipment failure."

b. APPA agrees with the change to use the EACS in the Applicable Systems column. We appreciate the fact that the EAMS are not included as we anticipate that they will be covered under other BCS-related standards. This provides another option to use the dual-definition approach and allow entities to select between either the existing EACM definition and requirements or use the new EAC/EAM definition and proposed new requirements.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	
Document Name	

Comment

abstain

Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	
Cowlitz supports APPA comment.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
a. Texas RE does not have an issue with the SDT adding CIP Exceptional Circumstances for Parts 1.8, 1.9, or R2. b. Please see Texas RE's response to #4 regarding the EACMS definition.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST.	

In addition, the SDT did not clearly demonstrate an added security benefit to these proposed changes that would justify the administrative burden and cost of implementation.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Removal of the allowance for CIP Exceptional Circumstance for R2 Part 2.1 and R2 Part 2.0 is a mistake. In the event of a physical emergency (e.g. fire, active shooter, chemical spill, etc.) the use of an escort likely will not be allowed by emergency personnel.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST supports the modifications related to CIP Exceptional Circumstances but opposes the exclusion of systems that perform electronic or physical monitoring.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	

ITC is in agreement with the comments submitted by EEI:

"In general, comments made in response to Question 11 also apply to our concerns with CIP-006."

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

In general, comments made in response to Question 11 also apply to our concerns with CIP-006.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 13.

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	No
Document Name	

Comment

CHPD is concerned about the overlap of CIP-005 R1 Part 1.2 and CIP-006 R1 Part 1.10. The protection of so-called "Super ESPs" seems to already be covered by the CIP-006 R1 Part 1.10. Only one of the requirements should be maintained, and given that CIP-006 R1 Part 1.10 is already in effect, it is CHPD's preference that it be maintained over CIP-005 R1 Part 1.2.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

In general, comments made in response to Question 11 also apply to our concerns with CIP-006.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

a. No. During an extreme weather event a CEC may be declared. For instance, if a tornado hit a substation and compromised the control building a CEC would be required for all of R1 not just the Parts in the proposed change. We recommend leaving the CEC at the R1 level.

b. No. We think that EAMS should also be afforded the same protections as EACS. It is a generally accepted security concept that if a person has physical access to a system it is difficult to prevent them from compromising that system. EAMS are an important part of providing security for BES Cyber Systems and should thus be afforded the same physical protections.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

a. Yes. Reclamation agrees with the modifications related to CIP Exceptional Circumstances. CIP Exceptional Circumstances are necessary during emergencies for first responders.

b. Reclamation supports adding systems that control access to the Applicable Systems column; however, Reclamation disagrees with the newly-proposed term EACS. Reclamation recommends the SDT use the term Intrusion Detection System (IPS) instead, as stated in the response to Question 4.

Reclamation recommends CIP-006 Requirement R1 Part 1.10 be changed

from:

Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:…

to:

Where physical access restrictions to such cabling, components, or Cyber Assets associated with communication networks and data communication links cannot be implemented, the Responsible Entity shall document and implement the following:…

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	

The removal NERC CIP Exceptional Circumstance language at the requirement level seems to be in opposition of the stated intent of the stated use of NERC CIP Exceptional Circumstance.

Standard emergency procedures seem to be disallowed by the inclusion of CIP Exceptional Circumstances at the sub-Requirement level and not at the Requirement level

We suggest that PACS and PAMS should be subject maintenance and testing per R3.1

Likes 0	
Dislikes 0	

Response

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

MEC does not agree with the conforming changes. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

a) No. During an extreme weather event a CEC may be declared. For instance, if a tornado hit a substation and compromised the control building a CEC would be required for all of R1 not just the Parts in the proposed change. We recommend leaving the CEC at the R1 level.

b) No. We think that EAMS should also be afforded the same protections as EACS. It is a generally accepted security concept that if a person has physical access to a system it is difficult to prevent them from compromising that system. EAMS are an important part of providing security for BES Cyber Systems and should thus be afforded the same physical protections

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

a. Agreed

b. The proposed definitions need to be re-evaluated and clarified before additional meaning full comments can be considered

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Support MRO NSRF comments

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	No
Document Name	
Comment	
Southern Company believes the CEC in CIP-006 R1.8 and R1.9, while helpful, only addresses logging failures. In a storm response mutual assistance situation, for example, you would still have to control, monitor, and alert on access, even if the entire PACS is lost, not just the logging function. With this situation, it seems that there are now less restrictions on visitors during a CEC in R2 than the employees who are on site repairing the system. Southern Company asserts that it will make more sense to move the CEC language to the higher level requirement level (R x) rather than the sub-requirement level (R x.y).	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	No
Document Name	
Comment	
a. During an extreme weather event a CIP Exceptional Circumstance (“CEC”) may be declared. For instance, if a tornado hits a substation and compromised the control building a CEC would be required for all of R1 not just the Parts in the proposed change. We recommend leaving the CEC at the R1 level. b. The SSRG believes that EAMS should also be afforded the same protections as EACS. It is a generally accepted security concept that if a person has physical access to a system it is difficult to prevent them from compromising that system. EAMS are an important part of providing security for BES Cyber Systems and should thus be afforded the same physical protections.	
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 no Dominion and NYPA	
Answer	No
Document Name	
Comment	
The removal NERC CIP Exceptional Circumstance language at the requirement level seems to be in opposition of the stated intent of the stated use of NERC CIP Exceptional Circumstance.	

Standard emergency procedures seem to be disallowed by the inclusion of CIP Exceptional Circumstances at the sub-Requirement level and not at the Requirement level We suggest that PACS and PAMS should be subject maintenance and testing per R3.1	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
a. Agree with the addition of CEC for the reqiuirement level of R2. Recommend it be maintain at the requirement level for R1. In the event of a catastrophic event an entitiy may have to declare a CIP Exceptional Circumstance that may require CEC all parts of R1. b. If EACMS is split into EAMS and EACS, what would be considered an EAMS? The camera systems or software used to perform electronic monitoring? CIP-006 only requires Electronic Control Systems (EACS) and no Electronic Monitoring Systems (EAMS). So an entity has to control access but does not have to monitor it, was this the intent of the SDT?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
In general, comments made in response to Question 11 also apply to our concerns with CIP-006.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No

Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
While we do not have any problem with the conforming modifications to CIP-006, we are still concerned about the other concepts that are driving the modifications as mentioned in our other comments.	
Likes 0	
Dislikes 0	
Response	

14. The SDT is proposing modifications to CIP-007 (see the CIP-007 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-007. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?

b. The SDT is proposing the security objective in CIP-007 R1, "to mitigate the risk posed by uncontrolled logical and physical connectivity". Do you agree that the modifications to CIP-007 R1 Part 1.1 fulfill this security objective for systems where connectivity is not limited to TCP/IP port service combinations, as in virtualized systems and SAN based storage?

c. Do you agree that the modifications to CIP-007 R1 Part 1.1 add necessary flexibility to fulfill the security objective of CIP-007 R1 for virtualized systems and provides a degree of future proofing?

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

a) Yes, the additions help clarify intent. As with any compliance standard, it is important to integrate the intent with the method of auditing to allow the intent to be the focus and not prescriptive details. This also needs to be clearly and consistently communicated throughout the regions.

b) Yes.

c) Yes.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

CIP-007-7, Requirement R1, Part 1.2 regarding the protection of unused physical ports. The Secure Configuration is not present in this Requirement and I believe it should be. The potential protections can be physical or logical, and a change could impact either one of these. For logical, it is easy to understand a change could change the logical setting of a port making it usable. For a physical change, a similar condition could occur of the change was the swap out of hardware and a physical port blocker was not re-installed or signage is not put back into place.

Likes 0	

Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP does not agree or disagree that the proposed security objectives add clarity to the reason the requirement exists. SRP also agrees the modification to CIP-007 R1 part 1.1 fulfills the security objective. Lastly, SRP agrees the inclusion of “other methods” provides the necessary flexibility.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
a. Agree b. Agree c. Agree	

Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP recommends diagrams to be included in the technical rationale to more clearly illustrate how the concepts controlling essential logical connectivity within the LIZ would be applied to new and virtualization technology.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Security objectives add clarity, but I would add the language “R1 is intended to limit the ability of an attacker to move laterally throughout the secure environment” from the Technical Rationale in the requirement itself.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Security objectives add clarity, but I would add the language “R1 is intended to limit the ability of an attacker to move laterally throughout the secure environment” from the Technical Rationale in the requirement itself.	

Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
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	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
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	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - 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	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following: The SDT should provide more clarity around scripts and installed software. In CIP 007-7 Requirement R2.1, how is “essential” defined? Is the intent of this requirement to prohibit authorized users from writing and executing scripts in the course of their work? Is there a timeframe for alerting on newly-installed software or executable scripts? What does installed mean? If an executable or script is copied to the system, is it considered installed? Is a for loop typed in a shell considered a script? Would a shell alias be considered a script?	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	

Comment
Button response should be "No". Button selection wasn't allowed. PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. The SDT did a good job here. PAC believes it allows the flexibility to develop the program based on the infrastructure and how the communications are managed. {C}a) The security objective concept isn't new to cyber security controls. However, the subjectiveness will make it hard to audit as entities develop different implementations. It could open up an issue when the auditors develop an approach that identifies certain methods are more desirable than others and suggest entities adhere to their opinions rather than the language of the standard. {C}b) Excluding serial communications works, PAC understands the reasoning behind the change. Concern here is on Ethernet capable devices that aren't being used (RTAC, SEL-411, etc.) "Configure each system to provide only essential logical connectivity" Will we need to disable and document the port on the Cyber Assets in the Medium BCS? {C}c) Yes.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	

Comment
Cowlitz agress with APPA comment.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	

Comment
APPA generally agrees that the proposed security objectives add clarity to the reason the requirement exists.

Public power does have some general concerns with CIP-007. With the removal of the TFE language, is guidance anticipated on “per system capability?” The removal of the, “with External Routable Connectivity” makes this important for registered entities to understand. Also, there are concerns that the “Detect and alert on malicious communication within systems,” included within the Requirement Part on Connectivity.

A further public power concern is: will vendor supported applications be able to provide sufficient documentation related to the implementation of the multiple elements of the “Secure Configuration?” If this does not exist in an application, will companies have sufficient time to procure/develop such a system prior to compliance date?

Another potential issue for public power will be determining what is the intent of the note related to Secure Configuration for the CIP-007-7 R3 Part 3.2 “Mitigate the threat of detected malicious code.” We understand that we need to remove or isolate the detected malicious code, but how does the removal become part of the Secure Configuration of the BCS? The capability to detect the malicious code will exist in the antivirus solution. Where else is it likely to become part of the implemented configuration? How does it apply to virtual environments?

Proposed CIP-007 and CIP-010, have significant cross references and requirements related to the documentation of the Secure Configuration. APPA recognizes that this will require significant resource commitment to manage security controls in a traditional and virtual/cloud-based environment.

The new requirement introduced in part R2 should be limited in applicability to virtualized BCS and associated PCS. No technical basis is evident to justify the expansion of scope to include this new requirement for the existing approach to securing non-virtual BCS, etc. Although this practice might be a good security practice, CIP requirements are intended to provide a baseline of security practices not a collection of all good or best practices. Indeed, there exist many other good security practices that are not included in CIP requirements. It is not sufficient justification alone to add a new requirement just because it is a good practice; there should exist an overriding technical or security need. If this requirement is maintained, we recommend that it apply to virtualized BCS only.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

a. Yes

b. It appears that TFEs are being eliminated, is that true? Will guidance be provided to better clarify “per system capability” and the expected compliance documentation? How will this be audited if device capabilities within a system vary, or if a system is not capable? Specific guidance for Secure Configurations should be included. If entities are required to develop, this could be timely. “Detect and alert on malicious communication within a system” seems to be better suited for either R3 or R4.

c. Yes

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy believes that a response to question #8 (regarding IP/Serial Converter inclusion in BCS) to fully comment. Are Secure Configuration items required to be documented? We believe the fifth bullet in R2.1 is too vague (Other methods?) and will allow for interpretation differences between the auditor and the Registered Entity. Also, the new verbiage now says “per system capability” instead of “where technically feasible” in CIP-007…Does that mean that an entity can retire filed TFEs as long as they maintain evidence of system capability? i.e. the entity does not have to perform material change tasks with the regions anymore.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO requests the SDT consider consolidating the requirements for Secure Configuration in a single Requirement or providing a Guidance Document.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
While we do not have specific comments on the questions proposed by the SDT, we do have concerns about certain updates within CIP-007. CIP-007 R1: For consistency, we suggest that the measure related to malicious commination under Part 1.1 be updated to include alerting or that alerting be removed from the requirement (“Detect and *alert* on malicious communication with systems”).	

CIP-007 R2: While we understand the reasoning behind the changes to R2, “controlling software that is allowed to execute on a BES Cyber Systems”, there is some confusion on what the requirement means. For example, what does “essential software execution” mean? As tedious as it might sound, adding words such as “essential” into the requirements without explicitly expressing what the intent of the word is, causes issues with the entities and the regions. It would be prudent to get away from words that can be construed in different ways or that can change the execution of the requirement depending on how they are interpreted. Additionally, treating scripts the same as software, without further explaining what types of scripts, will cause undue burden on entities. For example, is it the SDT intent that read-only scripts be tracked? We believe that this could turn into a time-consuming task that will never be completed to an auditor or the requirements satisfaction.

Additionally, the Secure Configuration concept is found throughout CIP-007. Please see our comment relating to Secure Configuration under question 15.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy would like to comment the SDT for the work done in CIP-007-6, as we believe a movement to a risk-based approach for security will allow the flexibility to develop the program based on the infrastructure and how the communications are managed. In addition, with the removal of the strict timelines for R2, this would alleviate the multiple violations of this Requirement due to missing the 35 day windows, versus the intent of a program in preventing any incident due to the lack of patching Cyber Assets.

a) NV Energy does recognize that this more flexible approach to security does have its difficulties. The increase in subjectiveness will make it hard to audit as entities develop different implementations. It could open up an issue when the auditors develop an approach that identifies certain methods are more desirable than others and suggest entities adhere to their opinions rather than the language of the standard.

b) Excluding serial communications works, NV Energy understands the reasoning behind the change. Concern here is on Ethernet capable devices that aren’t being used (RTAC, SEL-411, etc.) “Configure each system to provide only essential logical connectivity” Will we need to disable and document the port on the Cyber Assets in the Medium BCS?

c) Yes.

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	No
Document Name	

Comment

CIP-007 R1 Part 1.1's proposed wording appears ambiguous and confusing to us. The language of the requirement part does not contain the objective (where all of the other requirement parts in CIP-007 do contain the objective). Even though the security objective is present in the language of R1, it should be present in Part 1.1 as well, especially since R1.1 is after a page break.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	

Comment

While the revised CIP-007 R2 is appropriate, it should be included in CIP-010 and it is a component of configuration management.

Fullly support changes to requirement part 1.1, though additional guidance on how to demonstrate the requirement may be met is needed and agree that it will fill the objectives for virtualized systems.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	No
Document Name	

Comment

The structure of CIP-007 R1 requires mitigating risk of uncontrolled logical and phyicial connectivity which complicates the applicability table.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 14. Additionally, Westar | Kansas City Power & Light Company supplements the EEI response with the following observation: The proposed revision raises questions as to whether moving patching to CIP-010 will mean patching is to be part of the CIP-010 "vulnerability management program" and no longer part of Security Configuration / Baselines.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	

Comment
In general, comments made in response to Question 12 also apply to our concerns with CIP-007.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	

Comment
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI

Answer	No
Document Name	
Comment	
Although adding security objectives does allow for flexibility in the technical approach taken to comply it also poses additional potential for disparate interpretations of the requirement between entities and auditors. An approach the entity feels addresses the objective adequately may be viewed by the auditor as unsatisfactory. A more prescriptive model lends to more concise interpretation of the requirements.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
The structure of CIP-007 R1 requires mitigating risk of uncontrolled logical and phyicial connectivity which complicates the applicability table.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "In general, comments made in response to Question 12 also apply to our concerns with CIP-007."	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	

Answer	No
Document Name	

Comment

For Part 1.1, consider using “per system capability” instead of “excluding serial port connectivity such as RS-232 and RS-485.” Please clarify “Detect and alert on malicious communication within systems”. This basically calls for IDS at the hypervisor. Should this be in Requirement R3? Should this be something like limiting traffic? As written, Part 1.1 seems to imply that an entity would be required to implement all of the bulleted items if the system is capable. Please reconsider the wording of this. The note should not be used within requirement language in Part 1.1 and other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.

For Part 2.1, please provide clarification on executable scripts. This element continues to raise issues with disparate interpretations between entities and Regional Entities. A clear descriptor of this would aid in consistency of implementation across the industry. Consider using “available software” instead of “installed software”. There is software that can be usable without an actual installation process. Please clarify “essential”.

Regarding Parts 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 5.5, 5.6, and 5.7, the note should not be used within requirement language in Part 1.1 and other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST supports the idea of adding security objectives to top-level (“R”) requirements, but believes, for R2, that the SDT needs to provide at least a working definition of “managed software” before establishing an objective of mitigation risks posed by “unmanaged” software.

N&ST supports the goal of proposed R1 Part 1.1 modifications but believes that configuring applicable systems to permit only required logical/electronic communications should be mandatory, vs. only one of several acceptable options.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC disagrees with the magnitude of changes to this standard. By removing “with ERC” from the applicable systems column of the requirement tables, multiple requirements will be added to the audit scope that were previously not applicable if there was no ERC. The LIZ should only apply to the virtual devices.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST and NPDD.

In addition, the following questions should be addressed or guidance provided to address some ambiguity:

- CIP-007 R1.1
  - “Excluding port connectivity such as RS-232 and RS-485.” Should other exemptions be provided, such as DNP3 using non-routable? Or instance when data is carried over a TCP/IP network that are serial at the end-point. Stated differently, remove the specific exemptions and state serial communications are exempted.
  - Explain why “ERC” was removed from the applicability.
- CIP-007 R2.1
  - Does “to allow only essential software execution” exclude firmware?
  - Are manual methods of alerting allowed? Can alerting be done on a periodic basis, or does this requirement require real-time alerting?
- CIP-007 R3.2
  - Are we required to identify and document the mitigation processes used on a BCS process, or is this requiring each mitigation activity be part of the Secure Configuration? Currently reads as the latter which is a CIP-008 issue. In addition, including response activities within the Secure Configuration does not provide any value to detecting cyber security incidents.
- CIP-007 R5.1
  - For Interactive User Access, it could be a process or technical control. How should a process be documented as part of the Secure Configuration, especially if the process allows for different approaches / solutions?
  - Adding administrative overhead to track this / could result in creation of numerous new CSI documents which poses a risk.
- CIP-007 R5.2
  - Adding administrative overhead to track this / could result in creation of numerous new CSI documents which poses a risk.

- CIP-007 R5.3-5.5
  - No comments
- CIP-007 R5.6
  - How should a process be documented as part of the Secure Configuration, especially if the process allows for different approaches / solutions?
  - Adding administrative overhead to track this / could result in creation of numerous new CSI documents which poses a risk

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO

Answer	No
Document Name	

Comment

Please see MRO NERC Standards Review Forum (NSRF) comments.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5

Answer	No
Document Name	

Comment

PSE supports the comments developed by EEI.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	
Support MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
a. Agreed b., c. Need further review.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations. a) No. b) No. We do not see a need to change R1. We also are concerned with adding the "detect and alert" language to Part 1.1. Adding the detecting and alerting seems to be duplicative with CIP-010 Part 2.1. Adding the "detect and alert" language increases compliance obligations for Medium Impact systems.	

c) No. By adding this flexibility you also introduce auditor discretion into requirements that have very clear objectives. CIP-002-1 to CIP-002-3 required an entity to develop a Risk Based Assessment Methodology (RBAM) to determine Critical Assets. FERC did not agree with some entity assessments and requested the standard be changed to be more prescriptive. We now have the “Bright Line” criteria in CIP-002-5.1a. We think the risk assessment methodology provides the potential for relief of unnecessary burdensome work. The current requirements unintentionally require processes that do not make sense in certain circumstances but we think there is great risk of an auditor not completely understanding the entity’s risk and therefore issuing a PNC (Potential Non-Compliance).

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	AZPS Comments - Question 14.docx

Comment

Please see the attached document.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Security objective-based requirements may be the right direction, but at the wrong time. Other non-NERC standards that are security objective-based are not subject to zero-defect compliance monitoring. In this case, security objective-based requirements may provide too much flexibility that could result in too much difference in interpretation between different Responsible Entities and auditors. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	

Dislikes 0	
Response	
Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	
Adding the language to the Requirement does not make the Requirement objective based because the sub parts of the Requirement still need to be met.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	
Comment	
The proposed changes make progress toward accomplishing this goal, but they may also increase the compliance burden for existing BCS. Comments under question 9 apply here as well: The “ERC” qualifier has been removed from CIP-007 R1.1. This could dramatically increase burden on some entities, where the intended effect could be achieved instead with a virtualization-ready definition of “PCA” and “ERC.” CIP-007 R1.4 also seems to shift from requiring intrusion protection on an ESP level to requiring it on a BCS level. This will be onerous and may not be technically feasible in many cases, unless BCS are defined over-broadly (i.e., the entire LIZ is a single BCS). There is a meaningful distinction in keeping the BCS definition separate as a subcomponent of the LIZ. The appropriate shift would be from EAP to LIZ, not from EAP to BCS.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	

We disagree with these changes. We still support the current result-based requirements with appropriately prescriptive language. Even though the proposed objective-based non-prescriptive requirements provide some flexibility for the CIP compliance, they are too broad and subjective. By virtue of lack of detailed measures and guidance, how do the registered entities know their processes have been implemented effectively? How will Auditors/Teams be accredited to evaluate effectiveness? What will be the effectiveness metric? Given that currently the majority of CIP Cyber Assets are physical and the CIP compliance process today works fairly smoothly by implementing the existing requirements that are appropriately prescribed, it doesn't make sense to modify any existing requirements that are only for sufficing a small percentage of the virtual devices but a waste of the registered entities' time and resources for making these changes.

Resulting from our comments in the above question 1, as long as the virtual devices are identified correctly and the device-centric approach would still work well for the virtual devices, where the CIP-007 R1 Part 1.1 will apply to them smoothly.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

a. No.

b. No. The NSRF does not see a need to change R1. We also are concerned with adding the "detect and alert" language to Part 1.1. Adding the detecting and alerting seems to be duplicative with CIP-010 Part 2.1. Adding the "detect and alert" language increases compliance obligations for Medium Impact systems.

c. No. By adding this flexibility the SDT also introduces auditor discretion into requirements that have very clear objectives. CIP-002-1 to CIP-002-3 required an entity to develop a Risk Based Assessment Methodology (RBAM) to determine Critical Assets. FERC did not agree with some entity assessments and requested the standard be changed to be more prescriptive. We now have the "Bright Line" criteria in CIP-002-5.1a. We think the risk assessment methodology provides the potential for relief of unnecessary burdensome work. The current requirements unintentionally require processes that do not make sense in certain circumstances but we think there is great risk of an auditor not completely understanding the entity's risk and therefore issuing a PNC (Potential Non-Compliance).

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE does not agree CIP-007 needs to be changed with regards to virtual systems. Virtualized systems use ports and services just like physical systems and therefore they should all be evaluated and protected as they are currently. Texas RE has not seen issues specifically caused by virtualization using the current approach in CIP-007.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
We agree with some, but not all the modifications. We do agree that adding the security objectives in the requirements of CIP-007 is a step in the right direction. However, the requirements need to support defense in depth without penalty. For instance, in the modifications to CIP-007 R1.1, an entity can use a combination of four protections. If an entity employs two or more to an applicable system and one is found to have failed, then an Entity should not be found in violation if the other protection remained in place. The entity should only be found if violation if all protections for an applicable system related to R1.1 were not in place. Regarding modifications to CIP-007 R1.1, it is unclear if “Detect and alert on malicious communication within systems” actually meets the security objective of mitigating the risk posed by uncontrolled logical and physical connectivity. In addition, this is also a control for the security objective of mitigating the risk posed by malicious code in R3 and the security objective of monitoring security events to mitigate the risk posed by detectable security incidents in R4. So, if an entity chooses only this control for a system then they are potentially also in violation of R3.1 and R4.2.1. Either the mitigation measure needs to belong only to one security objective to avoid multiple violations if one fails, or the entire CIP-007 needs to be reworked to a program that addresses each risk and the entity has identified controls for each risk. Again, with the idea that an entity with multiple controls in place for a particular risk is not penalized when one control fails, but other controls remain in place. The proposed changes might provide a degree of future proofing, but per Master Yoda, “Difficult to see. Always in motion is the future.”	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	

Answer	No
Document Name	

Comment

No, NRG does not agree that adding the security objectives throughout the Requirements in CIP-007 adds clarity to the reason the requirement exists, because the new secure configuration definition mandates malware monitoring within BES Cyber Systems which implies AV on the BCS and not at the system level (which is the only requirement of the current standard). This proposed change could also imply needing network access control, whitelisting, and/or needing host based intrusion detection.

No, NRG does not agree that the proposed security objective in CIP-007 R1, “to mitigate the risk posed by uncontrolled logical and physical connectivity” because it expands the port control requirements. Registered entities that have used no ERC as a security measure,will now have additional compliance requirements. The security gained from these activities may not outweigh the additional compliance burden to the industry. NRG does not agree that the modifications to CIP-007 R1 Part 1.1 fulfill this security objective for systems where connectivity is not limited to TCP/IP port service combinations, as in virtualized systems and SAN based storage because The new secure configuration definition mandates malware monitoring within BES Cyber Systems which implies AV on the BCS and not at the system level (which is the only requirement of the current standard). This proposed change could also imply needing network access control, whitelisting, and/or needing host based intrusion detection.

No, NRG does not agree that the modifications to CIP-007 R1 Part 1.1 add necessary flexibility to fulfill the security objective of CIP-007 R1 for virtualized systems and provides a degree of future proofing because while the direction of the other version 7 standard revisions have shifted focus to a system, this requirement provides a vague approach with underlying expectation on cyber asset level protections. Many control system vendors do not currently support host-based firewalls and/or intrusion detection systems. The same protection could be realized at the system level through a combination of firewalls, intrusion detection, configurations monitoring, network access control, malware scanning, and TCA/RM controls.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

For Part 1.1, consider using “per system capability” instead of “excluding serial port connectivity such as RS-232 and RS-485.” Please clarify “Detect and alert on malicious communication within systems.” This basically calls for IDS at the hypervisor. Should this be in Requirement R3? Should this be something like limiting traffic? As written, Part 1.1 seems to imply that an entity would be required to implement all of the bulleted items if the system is capable. Please reconsider the wording of this. The note should not be used within requirement language in Part 1.1, or in other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.

For Part 2.1, please provide clarification on executable scripts. This element continues to raise issues with disparate interpretations between entities and Regional Entities. A clear descriptor of this would aid in consistency of implementation across the industry. Consider using “available software” instead of “installed software.” There is software that can be usable without an actual installation process. Please clarify “essential.”

Regarding Parts 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 5.5, 5.6, and 5.7, the note should not be used within requirement language in Part 1.1, or other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.

Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
In general, comments made in response to Question 12 also apply to our concerns with CIP-007.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST.	
Likes 0	
Dislikes 0	

Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	

In order to provide the necessary flexibility to fulfill the security objectives and to clarify ability to choose, please consider adding "or" at the end of each line of all bullet point lists providing options.

R1.1 recommended updated language reads:

• Configure each system to provide only essential logical connectivity; or

• Detect and alert on malicious communication within systems; or

• Baseline system logical connectivity, and alert on deviation from baseline; or

• Other method(s) to mitigate the risk posed by uncontrolled logical connectivity.

R2.1 recommended updated language reads:

• Configure each system with intentionally installed essential software and executable scripts; or

• Baseline currently installed software and executable scripts and alert on any newly installed software or executable scripts; or

• Implement application whitelisting; or

• Use read-only bootable media; or

• Other methods to mitigate the risk posed by unmanaged software.

Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

We disagree with the removal of “with External Routable Connectivity” as an applicable system in CIP-007.

Is CIP-007 R1 1.1 only applicable to systems where there is virtual technology? If so shouldn't that be listed as the applicable system? R1 is to mitigate the risk posed by uncontrolled logical and physical connectivity; Part 1.1 doesn't address physical and logical connectivity.

In CIP-007 2.1 – How would this apply to a BES Cyber System that is a System Protection Relay?

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 no Dominion and NYPA

Answer	No
Document Name	

Comment

Adding the language to the Requirement does not make the Requirement objective based because the sub parts of the Requirement still need to be met.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer	No
Document Name	

Comment

a. The SSRG requests the Standard Drafting Team ensure the language is clear enough to allow the Reponsible Entity to have clear direction what consistutes the type of port that is included in the Secure Configuration. For example, unlike CIP-007-6 which utilizes more concise language such as "logical network accessible ports that have been determined to be needed by the Responsible Entity…", version 7 utilizes terminology such as "only essential logical connecticity" and "uncontrolled logical connectivity," and states the standard excludes serial port connectivity "such as RS-232 and RS-485." This language appears very broad and subjective to what is included.

b. The SSRG does not see a need to change R1. Adding the "detect and alert" language to Part 1.1 seems duplicative of CIP-010 Part 2.1 and increases compliance obligations for Medium Impact systems.

c. The SSRG is concerned that by adding the referenced flexibility, auditor discretion is introducted into requirements that have very clear objectives. CIP-002-1 to CIP-002-3 required an entity to develop a Risk Based Assessment Methodology ("RBAM") to determine Critical Assets, which includes the "Bright Line" criteria in CIP-002-5.1a. The SSRG believes the RBAM approach provides for relief from unnecessarily burdensome work and mitigates auditor discretion.

Likes 0	

Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	No
Document Name	

Comment
MRO does not agree with these changes because it is not clear how “Mitigate the Risk” language supports enforceable requirements for the system security management of BES Cyber Systems. “Mitigate the risk” could be interpreted as anything between “Eliminate the Risk” and “Detect the Risk”. This could lead to challenges in consistent CMEP implementation by the ERO.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	

Comment
Southern Company requests clarification on the interplay between the objective in the overall requirement and the scoping of applicability in the table. As an example, CIP-007 R1 addresses mitigating the risk posed by uncontrolled logical and physical connectivity, yet the physical connectivity mitigation in the table is scoped to high impact control centers only. If an entity has only medium impact systems, what is the obligation of this requirement? The main requirement states they must implement a process that mitigates the risk posed by uncontrolled logical and physical security - and that plan(s) "collectively include" the requirement parts, but it does not state or clarify that it is *scoped* by those parts. This was not an issue previously as all the objectives and requirements were in the tables. It has changed now that the objective is in the overall requirement. Southern suggests the SDT consider this issue across all the standards and clarify how the high-level objectives work with the applicability column in the tables. Logical connectivity in CIP-007 R1.1 – does this unintentionally alter the scope for ports and services? This is a backwards compatibility question. Southern would like to see additional clarity in the definition for logical connectivity. This terminology is used throughout these proposed changes and clarity in the application of this term can provide clarity in scoping. Can this unintentionally scope in “anything connected to the system”? Will mounting a drive unintentionally scope in that logical connectivity? Do we have to start tracking (i.e. making lists) of everything that a system connects to? How might this extend into shared memory? Do we need to enumerate USB mice and keyboards?

Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	

15. The SDT is proposing modifications to CIP-010 (see the CIP-010 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-010. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?

b. The SDT is proposing to modify the referenced baseline configuration from CIP-010-3 R1 Part 1.1 to a 'Secure Configuration' which is made up of the implemented controls that fulfill requirements within CIP-005 and CIP-007. Do you agree that this set of controls supports managing change under CIP-010 R1 Part 1.1?

c. The SDT is proposing to modify the current CIP-007 R2 requirements and move them to CIP-010 R3. The SDT believes that the software vulnerability management found within this set of requirements fits logically within the security objective of CIP-010 R3 "to mitigate the risk posed by system vulnerabilities" and has moved it there. Do you agree?

d. The SDT is proposing CIP-010 R3 Parts 3.5 and 3.6 to replace the current CIP-007 R2 Parts 2.1 – 2.4. Do you agree that the proposed CIP-010 R3 Parts 3.5 and 3.6 offer the additional flexibility needed when implementing virtualized systems that can be dormant for a period, and for which security patches have become available?

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
We still recommend to provide a minimum required 12 month vulnerability assessment and not solely base it on risk for R3 Part 3.6	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the shift to risk-based implementation time frames.	
Likes 0	
Dislikes 0	
Response	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

a) Yes, the additions help clarify intent. As with any compliance standard, it is important to integrate the intent with the method of auditing to allow the intent to be the focus and not prescriptive details. This also needs to be clearly and consistently communicated throughout the regions.

b) Yes.

c) Yes.

d) Yes.

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Regarding b: Entities will need to track the Secure Configurations in a similar way to current baselines (with OS, software, etc) to monitor for and react to potential incidents and vulnerabilities. Additionally, tracking this way will assist entities in identifying, isolating and/or patching potentially vulnerable physical or virtual BCS.

Regarding d: This will require an entity to provide a thorough explanation of their rationale behind the periodicity for identifying software vulnerabilities.

Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

No comment.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

See previous comments regarding BCS and LIZ definitions

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3

Answer	Yes
Document Name	

Comment

In response to part C, Hydro One supports moving Patch Management program from CIP-007 to Vulnerability Management in CIP-010. Patches remediate vulnerabilities, but vulnerabilities can exist without a patch to remediate, so other mitigation maybe necessary.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment

Security Objectives do add clarity. Moving security patching to the Secure Configuration makes sense.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Security Objectives do add clarity. Moving security patching to the Secure Configuration makes sense.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
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	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
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	

Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

Button response should be "No". Button selection wasn't allowed.

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

The SDT did a good job here. PAC believes it allows the flexibility to develop the program based on the infrastructure and how the communications are managed.

{C}a) The security objective concept isn't new to cyber security controls. However, the subjectiveness will make it hard to audit as entities develop different implementations. It could open up an issue when the auditors develop an approach that identifies certain methods are more desirable than others and suggest entities adhere to their opinions rather than the language of the standard.

Secure Configuration (proposed) The implemented set of controls supporting the security objectives found within the CIP Reliability Standards where the following text exists within the requirement language: "NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system." New "Baseline" = CIP-005 R1.1, CIP-007

{C}a) R1.1, R2.1, R3.1, R3.2, R4.1, R4.2, R5.1, R5.2, R5.5, R5.6, R5.7, CIP-010 R3.6. This concept makes sense, but would need further review as compared to the original CIP-010 Bassline and CIP-007 controls documentation to fully understand the impacts of the changes proposed.

{C}b) From the beginning of CIPv5 that Patch Management should be CIP-010, PAC agrees with this change. Not understanding the new phrase "The process requirements of Part X.X and timeline are based on the analysis of the risks to BES reliability and the risks posed by the …". Is the SDT

expecting a risk register and program with thresholds of when things need to be done? Seems like this could be a good thing if we embrace this idea, but it leaves the auditors to determine what they feel is reasonable too when checking whether the timelines indicated line up with the risk level identified. Are there plans for future development during the drafting that the SDT plans to add some timeframes into the standards like before (i.e. every 35 days, etc.)

{C}c) Yes, PAC believes the SDT did a good job moving this to CIP-010 and allowing for flexible schedules based on system activity. However, our concern with timelines and risk are the same as explained in item “C” above.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

Public power agrees with transferring the requirements from CIP-007 to CIP-010 as mitigating software vulnerabilities more closely relates to vulnerability management rather than system management. However, as the 4 parts of this question suggest, these modifications add complexity to the standard. For example, the definition of the new term Secure Configuration and its role is unclear, and stakeholders can envision the term taking on more significance in the future. While it seems appropriate to identify the security controls as part of the Secure Configuration, some Entities had implemented the requirements for the current CIP-010 security controls by evaluating changes against all CIP-005 and CIP-007 security controls. Consequently, it would be best for the SDT to list out what the Secure Configuration is composed of.

APPA does consider that the move of the CIP-007 R2 requirements to CIP-010 is an improvement by locating them in a single standard. They are logically part of the methods that industry uses to mitigate the risk of system vulnerabilities. Further, we agree that the proposed changes will provide flexibility for virtual systems.

Although the Secure Configuration concept is not fully understood, either in application or audit approach, there is reasonable concern that it expands the scope of requirements for non-virtualized BCS. See further discussion above in responses to Question 14. Under the principle that CIP scope generally should not be expanded in these revisions for non-virtualized systems, the dual-definition/dual-requirement “overlay” approach discussed in Question 3, above, may be warranted as a means for entities to remove the scope expansion for existing BCS, for which the existing baseline approach may be sufficient.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	
Document Name	

Comment

abstain

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment

Cowlitz agrees with APPA comment.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

In addition, the following questions should be addressed or guidance provided to address some ambiguity:

- CIP-010 R1.1
  - Need to provide guidance on how timelines should be developed and what the risk analysis needs to consider. Is the entity required to develop their own risk analysis or will guidance be released making this more prescriptive? Will the resulting entity risk assessment process / criteria be subject to auditors?
  - Why does the requirement exclude EAMS and PAMS? Security controls should be applied to these systems that log and monitor. Not doing so will reduce security posture and make it difficult to meet requirements under CIP-006, 7 and 8.
- CIP-010 R1.2
  - Why is R1.2 written to CIP-005 and CIP-007 controls, whereas R1.1 is written to the Secure Configuration? This seems to be an inconsistency that should be addressed, or at a minimum explained.
- CIP-010 R1.3

- Is firmware and operating system exempted since it is not included within R1.3.1 and R1.3.2 requirement text?

- CIP-010 R2
  - Similar question on timelines. Also, why is impact rating called out in the bottom note when the only applicable impact rating is High Impact? How many different types of risk assessments need to be conducted across CIP-010?

- CIP-010 R3.5
  - Is software intended to include firmware and operating systems? Firmware and operating system is called-out in CIP-010 R1.3 but not here. Why the inconsistency?
  - Similar comment on conducting risk assessments. If 35-days was sufficient under CIPv5, is it also sufficient under this proposed revision, thereby not requiring a risk assessment?

- CIP-010 R3.6
  - Is software intended to include firmware and operating systems? Firmware and operating system is called-out in CIP-010 R1.3 but not here. Why the inconsistency?
  - Similar comment on conducting risk assessments. If 35-days was sufficient under CIPv5, is it also sufficient under this proposed revision, thereby not requiring a risk assessment?

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC disagrees with these changes. SMEC believes the change from Configuration Baseline to Secure Configuration and additional requirement for risk assessment exceed the mandate from the SAR and will be an unnecessary burden to industry. More detail on measures and guidance would be needed for such substantial changes.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment
N&ST supports the addition of various types of applicable system configuration data to what is presently referred to as a “baseline configuration.” However, N&ST opposes changing the name to “Secure Configuration,” as it would not, by itself, contribute to the goal of making BES Cyber Systems as resistant to attack as possible. What it would do, instead, would be to compel all Responsible Entities to overhaul their existing CIP-010 documentation. >> N&ST supports moving the existing CIP-007 R2 (patch management) requirements to CIP-010. N&ST also supports the goal of moving away from a calendar-driven, “apply all security patches” approach to vulnerability management. However, N&ST is concerned that some entities may lack the expertise necessary to perform comprehensive vulnerability management on an ongoing basis, and that among those that lack such skills, they could face tough questioning from audit teams. N&ST recommends adding some “… using one or more of the following approaches” language to the requirement language. An example might be, “By assigning security patching or mitigation action schedule priorities based on vulnerability severity ratings assigned by agencies such as the U.S. CERT.” N&ST is also concerned that while attempting to make CIP requirements generally less prescriptive, the SDT may have moved the pendulum too far: N&ST believes that allowing entities to to establish their own timetables for performing vulnerability identification and mitigation tasks incurs the risk of wide variations across the industry. N&ST has similar concerns about proposed changes to configuration monitoring requirements.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	No
Document Name	

Comment
The use of software throughout the Standard, like in 1.3, 3.5, and 3.6 is inconsistent with the requirements of R1.3 “operating system, firmware, and software”. Are we to assume that the term software actually means “operating system, firmware, and software”? Maybe a defined term is needed? The Secure Configuration definition is challenging us. Our preference woudl be that the definition did not referencing a set of standards, rather it were just fully defined. Also, we find this “NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system” text in CIP-010 R3.6 and I can’t trace back from that what the definition is.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	

Comment

The parts of Requirement R1 could be improved by putting the parts in sequence with actual change control (eg, implement in test, security controls testing, approve for production, etc.). As written the requirement is difficult to follow. The last statement in Part 1.1 should be guidance. It is not written as an objective requirement.

The last statement in Parts 2.1 and 2.2 should be guidance. They are not written as an objective requirement.

Requirement R3 is a good change over the current approach to patching. However, these changes may require significant significant capital investment and process changes. Requirement Part 3.6 should include provisions for changing a mitigation plan, similar to the current requirement in CIP-007 R2. This would allow entities to address changes in their timeline without the risk of a violation.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"EEI's concerns over the proposed changes to CIP-010 align with our comments and concerns as described for Questions 12."

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

The approach is good, but the scope and impact to existing operations is profound.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	No
Document Name	
Comment	
Although adding security objectives does allow for flexibility in the technical approach taken to comply it also poses additional potential for disparate interpretations of the requirement between entities and auditors. An approach the entity feels addresses the objective adequately may be viewed by the auditor as unsatisfactory. A more prescriptive model lends to more concise interpretation of the requirements.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon’s concerns over the proposed changes to CIP-010 align with our comments and concerns as described for Questions 12.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	

Answer	No
Document Name	
Comment	

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 15.

Additionally, Westar | Kansas City Power & Light Company share the following concerns.

Proposed Glossary Term, Secure Configuration, is ripe with compliance ambiguity and confusion. The Glossary Term can be interpreted as without boundaries. Recognizing flexibility in Standards and definitions is desirable, there is a need to provide a parameter, a fence, in which to operate.

Also, propagating into each CIP Standard is not required. Secure Configuration is restating a basic precept of compliance--establish and implement controls. Reiterating a fundamental principle of compliance does not promote compliant behavior nor improve reliability of the BES.

Finally, compliance ambiguity creates inconsistency in the CMEP.

Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	No
Document Name	
Comment	

The approach is good, but the scope and impact to existing operations is profound.

Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	
Comment	

Agree with additions to adding security objectives to CIP-010.

The definition of secure configuration is not adequately stated. This will either need to be fully prescriptive or fully non-prescriptive to be successful. While the fully non-prescriptive route would be preferred, this may result in an unenforceable standard.

Agree with moving CIP-007 R2 to CIP-010.

While conceptually supporting the changes, the details of how to comply with CIP-010 R3.5-3.6 are not adequately defined. Please provide clear guidance how to meet the standard and consider language changes to support the intent.

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	No
Document Name	

Comment

In general, as proposed, the Secure Configuration concept seems problematic The Secure Configuration now contains many new elements not previously tracked through the baseline configuration. Many of these additions are potentially difficult to inventory (for example, logging and alerting configuration may be distributed throughout multiple systems, such as local application configuration, AD Group Policy and SEIM configuration, which is spread across multiple asset classifications). Particularly with CIP-007 R4 and the changes to EACMS, some of these Secure Configuration items may be changes to non-applicable Systems (as SEIMs will in general be out of scope for CIP-010 R1, but the BES Cyber System's configuration for logging and alerting, which is required to be part of the Secure Configuration, will reside on this out of scope device).

Several of the requirements (CIP-007 R3.2 and the procedural aspects CIP-007 R5.5 and R5.6) are procedural in nature. It does not make sense to include these in a Secure Configuration, as the actual configuration of the associated system is not changing when a change to these procedures is made.

Additionally, some of the requirements (CIP-007 R5.1 and CIP-007 R5.2 marked to be part of the secure configuration seem at best redundant. These items rarely change, and usually not at the behest of the Responsible Entity, RE, (the methods of authentication rarely change from deployment; changes to the default account inventory are usually due to a vendor disclosure of an undocumented account). As such, it does not really make sense to include these in the Secure Configuration, requiring regular monitoring and inventory.

In CIP-010 R3.6, the requirement allows for other means to mitigate a vulnerability besides the installation of security patches. This would now require CIP-010 change control for changes that might be covered by other CIP requirements (requirement not already part of the secure configuration), or even outside the standards. This greatly increases the burden of CIP-010 R1 on REs.

Another problem with the current proposal is that the way the "Secure Configuration" tag is applied to the requirements can be ambiguous. For example CIP-010 R3.6, which requires the RE to "Create or update a plan to mitigate the identified software vulnerabilities…" includes the Secure Configuration tag. The question becomes is the plan part of the Secure Configuration, or the security patches/mitigations implemented? Once again, procedural methods may fall into the scope of the Secure Configuration.

Finally, the SDT suggests in the Rationale that the expansion the of Secure Configuration beyond the currently implemented items in CIP-010-2 R1 Part 1.1 is needed due to the greater risks posed by virtualization. Yet there is no accounting for risk for purely physical systems, and potentially the compliance burden might even be higher given the lack of a centralized management platform on physical systems. This would place an undue burden upon entities who choose to remain physical rather than adopt the complexities of virtualization

CHPD would like to see the removal of the Secure Configuration tag from CIP-007 Requirement Parts R3.2, R4.1, R4.2, R5.1, R5.2, R5.5, and R5.6. Additionally, CHPD would like the Secure Configuration to be made more granular to only apply to actual configuration on applicable systems for all requirements (such as installed patches for CIP-010 R3.6 or local configuration changes).

CHPD support the changes moving CIP-007 R2 to CIP-010 R3.5 and R3.6 as well as the changes made (with the exception of the Secure Configuration tag).

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

CenterPoint Energy supports the flexibility of the timeframes being determined by Entity. However, below are questions that need clarification:

- Where is the line between changes required for incident response and the change control process required in CIP 010-4 Requirement R1?
- Is authorization required prior to the remediation step in an incident response plan?
- The CIP 010-4 Requirement R1.1 requirements may have the inadvertent impact of slowing down incident response. Can IR policies be customized to pre-authorize remediation changes?

The removal of Requirement R1.2 requiring authorization without reference to timeframe may hinder timely incident response. With this new change, entities are tied to pre-authorization of any change and potentially penalized for acting in response to operational or security circumstances.

Changes to CIP-010 Requirement R1.3 do not exclude installation of signatures addressed in CIP-007 Requirement R3. While it is important to validate software, this requirement may impede timely implementation of signature based security controls even more than the current CIP-007 Requirement R3 requirements do. This entity recommends excluding signatures in this requirement to allow entities the flexibility to automate signature updates without retaining records of hash verifications for each transaction.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does recognize that this more flexible approach to security does have its difficulties. The increase in subjectiveness will make it hard to audit as entities develop different implementations. It could open up an issue when the auditors develop an approach that identifies certain methods are more desirable than others and suggest entities adhere to their opinions rather than the language of the standard.

NV Energy is unable to provide a effective evaluation for this question at this time, due to the extent of the “Secure Configuration” spanning multiple Requirements in CIP-005 and CIP-007. Further review will be needed to determine the impact of this new model.

NV Energy would like to comment the SDT for the work done in CIP-010, as we believe a movement to a risk-based approach for security will allow the flexibility to develop the program based on the infrastructure and how the communications are managed. In addition, with the removal of the strict timelines from CIP-007-6 R2, and moving to a risk based approach for review in CIP-010, this would alleviate the multiple violations of this Requirement due to missing the 35 day windows, versus the intent of a program in preventing any incident due to the lack of patching Cyber Assets.

NV Energy does agree with this approach for addressing virtualized systems in CIP-010 R3, P3.5 and P3.6

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

a. We agree that the proposed security objectives add clarity to the reason the requirement exists.

b. While we agree with the SDTs approach to not include the long list of requirements associated with Secure Configuration in the definition or in CIP-010, we do not agree with the concept of Secure Configuration. The move from Version 3 to CIP Version 5 saw the elimination of almost all of the “spaghetti requirements” with the expectation of CIP-010 R1, which, in essence, was just a documentation exercise. This was a welcome change and eliminated a lot of confusion. The addition of the Secure Configuration concept, and the combined 13+ parts, feels like the industry is going backwards and not forwards. In short, this is a documentation nightmare that has no benefit for the entities or the BPS. Furthermore, tracking and monitoring several of the items within the Secure Configuration seems time intensive or not feasible. We propose that the SDT continue to consider how CIP-010 could become a more objective-based reqruiement, instead of the currently proposed prescriptive-based requirement, and also focus on eliminatating the risk associated with creating “spaghetti requirements” and the administrative burden that comes with an inordinate amount of compliance documentation without a security benefit.

c. While we agree that focusing on software vulnerabilities is an improved approach, we believe that the requirement as written can cause additional confusion. For example, if an entity’s program is based on security patches and there is a software vulnerability that has been publicized and yet has no associated security patch, is the entity required or expected to implement a “plan to mitigate the identified software vulnerability”? We believe as written, the entity could say no to the question above (there is no patch therefore they have not identified a vulnerability) but an auditor could argue that they are out of compliance. Additionally, focusing on just software vulnerabilities could lead some entities to feel pressure to apply “hot fixes” to their environment which could cause severe reliability issues for the BPS.

Likes 0	

Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	

Comment
It doesn't appear there is a requirement to document the Secure Configuration. Is this the case? Is R1.1.1 requiring Authorization prior to the change being implemented? Should R1.3 be implemented Secure Configuration instead of existing? R2.1 – What is the difference between Configuration monitoring and Configuration auditing? R3.3 – R3.2 allows for "per Cyber Asset capability" but R3.3 does not. Without timeframe expectations in R3, the opportunity for interpretation differences between the auditor and RE may exist.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
It makes sense to move CIP-007 R2 to CIP-010. The elimination of the 35-day timeframe requirement for patching and moving toward a risk-based assessment methodology, while makes sense, poses concerns about how this will be audited. The risk in allowing entities to manage vulnerabilities based solely on risk may alter accountability in assessing and applying patches in a timeframe viewed acceptable by auditors.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3,5	
Answer	No
Document Name	

Comment
AEP is in agreement with the concept of raising the Requirements to an objective level. However, we have concern for the proposed movement of the vulnerability management requirements from CIP-007 to CIP-010. Our belief is that CIP-010, as it is today, is essentially a quality assurance standard

established as a means for confirming all the vulnerabilities “have been managed” not for requirements “to manage” vulnerabilities. AEP requests that the SDT consider retaining CIP-010 in this role by returning proposed CIP-010-4 Requirement Parts 3.5 and 3.6 to their former place in CIP-007. And, AEP requests specific examples of the intended implementation of ‘Secure Configuration’ be included in the technical rationale to provide more clarity of how this concept will reduce administrative burden in complying with the CIP standards.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to “what to do” not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

a. No.

b. Yes. However, this change will increase the number of Cyber Asset attributes that need to be tracked for what was previously baseline attributes and will increase the compliance risk for change control. For instance, if a new generic account is added to a Cyber Asset (common operator account), current requirements are to identify and inventory the account. The proposed requirement makes this part of the Secure Configuration which will require the addition of the account to follow CIP-010-4 Part 1.1 change control processes. Currently, following your CIP-010-2 change control process is a best practice; it is not a violation if you do not follow it when adding a new generic account. This is just one example. Creating the new Secure Configuration definition and tying the definition to CIP-010-4 will significantly increase compliance work and introduces concern with auditor discretion.

c. No. We don’t think it matters which standard, CIP-007 or CIP-010, the requirements reside. Moving the requirements will cause unnecessary documentation changes.

d. No. We think the new requirements add the ability for auditor discretion to requirements that were previously very clear. For instance, if an entity chooses to only monitor patch sources (Part 3.5), it would reason that if no security patches are released there would be no requirement to have a mitigation plan. However, if an entity chooses to monitor patch sources as well as monitor a vulnerability database (Part 3.5), a mitigation plan would be required if a vulnerability is discovered in the database even though there is no patch released for the vulnerability. An auditor may view this as a weak program and issue a PNC.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	

We disagree with these changes. We still support the current result-based requirements with appropriately prescriptive language. Even though the proposed objective-based non-prescriptive requirements provide some flexibility for the CIP compliance, they are too broad and subjective. By virtue of lack of detailed measures and guidance, how do the registered entities know their processes have been implemented effectively? How will Auditors/Teams be accredited to evaluate effectiveness? What will be the effectiveness metric? Given that currently the majority of CIP Cyber Assets are physical and the CIP compliance process today works fairly smoothly by implementing the existing requirements that are appropriately prescribed, it doesn't make sense to modify any existing requirements that are only for sufficing a small percentage of the virtual devices but a waste of the registered entities' time and resources for making these changes.

Resulting from our comments in the above question 1, as long as the virtual devices are identified correctly and the device-centric approach would work well for the virtual devices, where all existing requirements of CIP-007 and CIP-010 will apply to them smoothly.

Likes 0	
Dislikes 0	
Response	

Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	
Comment	

The new CIP-010 provides a logical configuration control framework that can be extended to cover future Requirements without requiring a revision of CIP-010. The proposed changes do significantly increase the scope of configuration change control. However, this increase in scope may not be entirely onerous; management controls corresponding to the Secure Configuration already need to be implemented in some form to ensure compliance with the corresponding Requirements.

While the new language does provide flexibility, some of that flexibility comes with compliance uncertainty. Where process requirements and timeline are based on risk analysis, significant additional definition is needed around what is acceptable for a risk analysis and how it shall be determined; this language leaves the door wide open for entities to give themselves the broadest interpretation of the gray area internally, resulting in unresolvable disagreements upon audit.

To provide reasonable assurance, a separate Requirement or even a separate Standard may be required for defining risk analysis, similar to how CIP-002 defines Impact Rating. A clear distinction may need to be drawn between Impact Rating and risk analysis.

As an alternative, a collaborative process may need to be formally defined and required outside of the audit process, in which the risk analysis methodology is reviewed and approved by the RRO, and the analysis itself may require a form of interaction with the RRO.

Likes 0	
Dislikes 0	

Response	
Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	
Moving to a security objective approach implies for a need for a cyber-security plan which considers the risk and appropriate mitigation and controls to meet the objective.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
Security objective-based requirements may be the right direction, but at the wrong time. Other non-NERC standards that are security objective-based are not subject to zero-defect compliance monitoring. In this case, security objective-based requirements may provide too much flexibility that could result in too much difference in interpretation between different Responsible Entities and auditors. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues. It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
a. Agree b. Agree c. Agree d. Disagree. The question d) seems to indicate that the intention of the SDT is that patches must be applied to dormant systems. This might not be desired if dormant instances are serving as backups to a production instance (for CIP-009 purposes). Flexibility is needed to allow for dormant intances/ systems to remain as is and only apply patches if the dormant instance is reused as a production instance (CIP-010 R1.2).

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	AZPS Comments - Question 15.docx

Comment
Please see the attached document.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	

Comment
NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations. a)No.

b) Yes. However, this change will increase the number of Cyber Asset attributes that need to be tracked for what was previously baseline attributes and will increase the compliance risk for change control. For instance, if a new generic account is added to a Cyber Asset (common operator account), current requirements are to identify and inventory the account. The proposed requirement makes this part of the Secure Configuration which will require the addition of the account to follow CIP-010-4 Part 1.1 change control processes. Currently, following your CIP-010-2 change control process is a best practice; it is not a violation if you do not follow it when adding a new generic account. This is just one example. Creating the new Secure Configuration definition and tying the definition to CIP-010-4 will significantly increase compliance work and introduces concern with auditor discretion.

c)No. We don't think it matters which standard, CIP-007 or CIP-010, the requirements reside. Moving the requirements will cause unnecessary documentation changes.

d)No. We think the new requirements add the ability for auditor discretion to requirements that were previously very clear. For instance, if an entity chooses to only monitor patch sources (Part 3.5), it would reason that if no security patches are released there would be no requirement to have a mitigation plan. However, if an entity chooses to monitor patch sources as well as monitor a vulnerability database (Part 3.5), a mitigation plan would be required if a vulnerability is discovered in the database even though there is no patch released for the vulnerability. An auditor may view this as a weak program and issue a PNC.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

: a. Agreed

b., c., d. Need further review.

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP does not agree or disagree that the proposed security objectives add clarity to the reason the requirement exists. SRP agrees with transferring the requirements from CIP-007 to CIP-010 as mitigating software vulnerabilities more closely relates to vulnerability management rather than system management.

However, SRP asserts the Secure Configuration definition needs more clarification. To understand the components of Secure Configuration, Responsible Entities would need to sift through the requirements. It should be clearly stated in the definition what the Secure Configuration is composed of.

Likes 0	
Dislikes 0	

Response

Jamie Prater - Entergy - 5,6

Answer	No
Document Name	

Comment

Entergy feels that the proposed changes to CIP-010 increase the scope of CIP-010 to an extent where those changes may be redundant with other requirements such as CIP-005-7 R1.1, CIP-007-7 R1.1, R2.1, R3.1, R3.2, R4.1, R4.2, R5.1, R5.2, R5.5, R5.6 AND R5.7. These redundancies would need to be resolved by modifications to or eliminations of those other requirements.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Support MRO NSRF Comments

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No

Document Name	

Comment

Southern Company generally agrees with the direction, but has several concerns. One area in which we would like clarification is regarding the "analysis of risk to the BES" or the system. Does this analysis need to be performed and documented on a per patch basis? On a vulnerability basis? Can entities create processes for system analysis with standard categories that have appropriate timeframes associated with them?

Southern is also concerned with the "Secure Configuration" which could end up being a vast number of methods on various systems and is no longer bound to five discrete software change categories. Proving proof of change management on every change to any kind of "method" throughout CIP-005 and CIP-007 will be challenging if not impossible.

For Part R3.6 Southern would like clarification stating that existing mitigations may be sufficient for the risk of a particular vulnerability and the entity may not have any further analysis or mitigation required because of these existing mitigations. In other words, past applied compensating controls may also cover many future vulnerabilities. It needs to be clarified that this situation is either A) not an applicable vulnerability in part 3.5, or B) it is, but nothing FURTHER needs to be done in 3.6. Southern prefers option A.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer	No
Document Name	

Comment

Generally, it is not clear why the proposal is to move away from the concept of an undefined baseline configuration to the "Secure Configuration." The new requirements in Parts 3.5 and 3.6 of CIP-010-4 are less prescriptive than what is being replaced from CIP-007, and appears to allow a more subjective approach for determining the timeline and periodicity for identifying vulnerabilities. The SSRG recommends the Standard Drafting Team review the draft to ensure its objectives are being met.

Specific to "b" - this change will increase the number of Cyber Asset attributes that need to be tracked from what was previously considered baseline, and will heighten the compliance risk for change control. For instance, when a new generic account is added to a Cyber Asset (common operator account) the current requirements provide for identification and inventory. The proposed requirement makes a new generic account part of the Secure Configuration and will require the CIP-010-4 Part 1.1 change control processes. Currently, following the CIP-010-2 change control process for a new generic account is a best practice but not a violation. This is just one example where the proposal is not backwards compatible. Creating the new Secure Configuration definition and tying the definition to CIP-010-4 will significantly increase compliance work and introduces auditor discretion.

Specific to "c" the SSRG doesn't think it matters whether CIP-007 or CIP-010 houses the requriements. However, the real issue is the uneccesary documentation changes that will be required to move the language; therefore, the drafting team may consider whether moving the requirements to CIP-010 is the most efficient means to address the issues.

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 no Dominion and NYPA	
Answer	No
Document Name	

Comment
Moving to a security objective approach implies for a need for a cyber-security plan which considers the risk and appropriate mitigation and controls to meet the objective.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	

Comment
The introduction of the new term Secure Configuration and its role is unclear. The proposed security objective throughout the Requirements in CIP-010 does not offer any clarity. For example removing the 35 day requirement for patching leaves it open to an auditor's interpretation of what they think is appropriate. Also, in CIP-10 R3, 3.5 the following sentence needs clarification and guidance: "The process of Part 3.5 shall include the periodicity for identifying software vulnerabilities based on the risk to BES reliability and the impact rating of the applicable system(s)."

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	

Comment
Regarding subquestion B, Tri-State requests clarification on the control change process outlined in CIP-010 R1.1, specifically the language in R1.1.2 "could be impacted by the change." Is the intention of this requirement for each entity to make a determination of what could be impacted, or is the

intention that each of the Secure Configuration components throughout these changes in CIP-005, CIP-007, and CIP-010 are the universe that must be considered?

Additionally, in CIP-010 R1.2.1 would like clarification of what specifically is included as "required" in the language "to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected"

Regarding subquestion B and the components of Secure Configuration, Tri-State requests that CIP-007 R3.1. and R3.2 are updated with language to require these sub-parts only if the system is capable.

CIP-007 R3.1 recommended updated language reads: "Deploy method(s) per system capability to deter, detect, or prevent malicious code"

R3.2 recommended updated language reads: "Mitigate the threat of detected malicious code, per system capability."

Regarding subquestion C, Tri-State recomends adding "or" after each bullet (similar to recommendations in Question 14). This language will clarify the ability to choose from the list.

CIP-010 R3.5 recommended updated language reads:

• Vulnerability database monitoring; or

• Patch source monitoring; or

• Vulnerability scanning; or

• Other method(s) to identify software vulnerabilities.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI’s concerns over the proposed changes to CIP-010 align with our comments and concerns as described for Questions 12.

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The parts of Requirement R1 could be improved by putting the parts in sequence with actual change control (eg, implement in test, security controls testing, approve for production, etc.). As written the requirement is difficult to follow. The last statement in Part 1.1 should be guidance. It is not written as an objective requirement. The last statement in Parts 2.1 and 2.2 should be guidance. They are not written as an objective requirement. Requirement R3 is a good change over the current approach to patching. However, these changes may require significant significant capital investment and process changes. Requirement Part 3.6 should include provisions for changing a mitigation plan, similar to the current requirement in CIP-007 Requireemnt R2. This would allow entities to address changes in their timeline without the risk of a violation.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
No, NRG does not agree that adding the security objectives throughout the Requirements in CIP-010 adds clarity to the reason the requirement exists because: The changes to CIP-010 change the understood intent of the standard from Change Control to a hybrid objective. A recommendation would be to change the standard to “Vulnerability Management” and realign the requirements with the new objective. No NRG does not agree with the proposal to modify the referenced baseline configuration from CIP-010-3 R1 Part 1.1 to a ‘Secure Configuration’ which is made up of the implemented controls that fulfill requirements within CIP-005 and CIP-007 and that this set of controls supports managing change under CIP-010 R1 Part 1.1 NRG asserts that the requirement changes while reducing overall compliance burden, introduce a new “spaghetti” requirement. NRG recommends that a specific list of Secure Configuration, even as an addendum, would be helpful. No, NRG does not agree with the proposal to modify the current CIP-007 R2 requirements and move them to CIP-010 R3 and does not believe that the software vulnerability management found within this set of requirements fits logically within the security objective of CIP-010 R3 “to mitigate	

the risk posed by system vulnerabilities" because the intent of CIP-007 patch management requirements were readily understood by the industry, while developing a risk based system is left to the interpretation of each Registered Entity. The result is going to be a large disparity in patching cycles between entities and even within the same entity. This will make auditing & benchmarking more difficult and could lead to industry difficulty with implementation of standards change.

No, NRG does not agree that the proposal of CIP-010 R3 Parts 3.5 and 3.6 to replace the current CIP-007 R2 Parts 2.1 – 2.4 offers the additional flexibility needed when implementing virtualized systems that can be dormant for a period, and for which security patches have become available because in relation to virtualized systems, NRG asserts that the proposed requirements do offer flexibility. However, there is no prescriptive criteria to manage the duration of dormant periods.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

While we agree with adding the security objective to the requirements it appears that a security objective was not added to R4.

We believe that the relocation of CIP-007 R2 to CIP-010 R3 makes much more sense and allows for Entities to finally address vulnerabilities as part of compliance and not just potentially wasted effort on patches which are only a component of vulnerability management. In addition, Entities now can get compliance credit for addressing vulnerabilities when announced rather than waiting for patches which may lag the vulnerability announcement by months. However, the concept of revising a vulnerability mitigation plan in CIP-007 R2.4 does not appear to have been ported to the CIP-010 R3 modifications.

While we appreciate the SDT trying to revise CIP-010 R1 for the better, it is currently a chicken and the egg requirement. The requirement states, "Control change to the Secure Configuration" and "Prior to the change determine required cyber security controls in the Secure Configuration that could be impacted by the change." So, if we are to control change to the Secure Configuration then we need to know what will change and yet we are to take an educated guess as to what in the Secure Configuration COULD be changed. Also, the question is prior to what change? The previous requirement was changes to the Configuration Baseline. We would recommend that the impetus for change management should still be defined as a change to Operating System, or firmware where not OS exists, change to software versions, and the application of all patches not just security patches. Changes to logical network accessible ports should be dropped from the list of items that prompt a change given the modified CIP-007 R1.1 controls. If necessary, these change triggers could be defined as Configuration Change. However we believe the concept of Configuration Baseline can be dropped in favor of a Secure Configuration. Tracking the Configuration Baseline is no longer required when the modifications to CIP-007 R2 address the security objective of unmanaged software. Also, it is unclear when CIP-010 R1.3 would be triggered if the impetus is a change the Secure Configuration and not a Configuration Change. If an entity implemented application whitelisting for CIP-007 R2.1 then would CIP-010 R1.3 ever be triggered? The impetus is a change that deviates from the Secure Configuration. If application whitelisting remains implemented when the OS, firmware, software (or patch) is installed or updated then did the Secure Configuration ever change? If not, then an entity doesn't have to perform either of the verification tasks. Therefore, the impetus for any CIP-010 R1 change should be a Configuration Change like before, but without tracking the Configuration Baseline.

We have concerns regarding the monitoring of the implemented Secure Configuration in CIP-010 R2. First, we have implemented Device Specific Test Plans for many types of Cyber Assets for the current CIP-010 R1. While many aspects of the Secure Configuration can be monitored through configuration monitoring, many still require the inspection through configuration auditing which is more time consuming for personnel. In addition, unauthorized change to the Secure Configuration could be considered a system vulnerability and should potentially be managed under that security

objective. If it is managed under R3 then it should be only performed if monitoring of a Secure Configuration property has not occurred in X amount of time. This is because many of the Secure Configuration properties would be inspected throughout the year as part of the change management process.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro's view is that the inclusion of serial port configuration in the Secure Configuration is too broad and may not be manageable relative to the risk posed. Also, it seems unclear whether USB ports would be considered in scope.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE does not agree CIP-010 needs to be changed with regards to virtual systems. Virtualized systems should be baselined just like physical systems as they are currently done. Texas RE has not seen issues specifically caused by virtualization using the current approach.	
Likes 0	
Dislikes 0	
Response	

16. Provide any additional comments for the SDT to consider, if desired.

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	
Document Name	

Comment

Clarification for the CIP-010-4 R1.2 term "models" would be valuable. This is an ambiguous term that in current standards provides confusion for what will satisfy expectations. We see this as possible via formalizing the term with definition, stating more clear aspects, or including specific guidance in the supporting documentation of the standard.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	
Document Name	

Comment

First, MISO would like to thank the SDT for their efforts in drafting these revisions. Revising existing CIP Standards is a difficult task and MISO appreciates the quality of the proposed changes and the effort put forth by the Team. MISO is encouraged by the work to modernize the standards and recognize that many modern software and hardware configurations are capable of safely and securely separating BES and non-BES workloads on the same physical hardware. The move to LIZ that is not focused on a subnet centric design is welcome. The changes to a risk based approach to patching instead of a hard time limit is also encouraging, however guidance will need to be provided on what will be required when audited to ensure that the risk criteria and decisions made around patching are appropriate and compliant.

The proposals do raise some questions with MISO around data protections for data in transit, as well as the definition of "secure configuration" and what may need to be demonstrated for that requirement.

The proposed changes do not yet tackle in any way the use of "cloud" or off-prem providers who would have continual management connectivity into the environment for CIP computational or storage workloads. They also do not yet address handling certain types of CIP data using Cloud storage providers.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Overall, we support changing from prescriptive-based requirements to objective-based requirements and most of the concepts presented to help clarify virtualization in the CIP environment. However, aside from the concerns mentioned throughout, we do have some concerns on how the updated requirements will be audited. Specifically, how will the auditors apply the requirements to entities that have no virtualization or entities that have their virtual environments segmented (i.e. one virtual environment for high impact BES Cyber Systems, one virtual environment for associated high impact EACs, one virtual environment for associated high impact PACS, etc.)?

We are also in support of EEI comments.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

In the development of NV Energy comments, we have struggled with trying to find some middle ground that acknowledges the hard work and laudable efforts made by the SDT, unfortunately, the structure of the comment format did not lend itself to such comments.

Nevertheless, NV Energy cannot support the level of change being proposed at this time, due to the recognition that virtualization remains a small piece implemented within the industry, and will continue as such for the foreseeable future. This has led us to the conclusion that SDT efforts need to focus more on the how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption.

NV Energy does not support the overly broad and sweeping change proposed by the SDT because it is premature. While there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time would prove to be too disruptive to existing efforts by the industry. Furthermore, there is limited acceptance of virtualized networks within the industry and efforts to try and tailor the current body of standards to accommodate this emerging security solution is likely to create needless security concerns. Instead the SDT should work toward addressing the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized environment using the existing body of standards, as currently approved. We further believe that the level of change being considered by the SDT would be better addressed through a separate initiative spanning several years to allow more engagement by the industry.

NV Energy also notes that while the SDT has offered up some very interesting ideas to address virtualization within BES Cyber Systems, many Responsible Entities still feel there is a lack of overall clarity necessary to address the design, control, and protection of these systems in a virtualized environment.

NV Energy's last concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, we are concerned that from an audit perspective this approach may prove to be very difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effective and consistently audited.

Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
CenterPoint Energy supports EEI's comments and approach for the next steps to address virtualization. It is important to highlight that these revisions were not mandated by a FERC order. Furthermore, entities with virtual environments are already complying with the existing CIP standards. In order to address virtualization and other emerging technologies, CenterPoint recommends that the SDT focus its efforts in transferring these concepts to Implementation Guidance or through a separate inititive to allow more engagement by the industry While the proposed revisions offer some flexibility for implementation, CenterPoint Energy is not in favor of the level of changes being proposed by the STD team at this time. The large fundamental changes proposed in this draft may introduce potential unintended consequences and challenges with auditability at a time when the industry is affirming compliance with the current version of the CIP standards. If the SDT continues to proceed with these revisions, CenterPoint Energy recommends addressing the items commented above and conducting implementation pilots to surface implementation challenges, similar to what was done with the CIPv5 pilots.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	

Document Name	
Comment	
Wabash Valley thanks the SDT for the hard work to meet a difficult and evolving challenge. As this appears to be a total redo of large parts of the standard, the SDT should consider that techniques similar to those used in the implementation of version 5 of the standard may be required to fully flesh out the revisions, preferably prior to final approval of the new standard.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	
Document Name	
Comment	
We urge the drafting team to implement this in stages and consider the EACS/EAMS and PACS/PAMS changes initially. These changes will have the least operational impact and the greatest security benefits. Introduction of secured configuration and CIP-005 changes should be transitioned over time to reduce operational risk and impact.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 16.	
Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	

Seattle City Light recognizes the complex and difficult job the SDT had in drafting the proposed virtualization standards, and applauds the persistence and creativity shown in crafting the present proposal. We appreciate these efforts. Project 2016-02 provides best practices for security standards that strive to stay ahead of adversaries' efforts. The Project is groundbreaking and is the first step toward the next level of the best practices in security standards. We see this effort to date as significant progress.

Importantly, refining and implementing the virtualization standards will be a challenge for NERC and industry. Seattle suggests the following as general principles that might guide futher development of the the proposed virtualization changes:

We strongly support for direction of proposed changes, as very promising and necessary to accommodate technological change and increasing theats

That said, the changes proposed are more far-reaching than expected, likely have many unintended consequences, are in some areas complex and largely untried, and in other cases expand the CIP scope to address new vulnerabilities introduced by virtualization

Therefore, Seattle recommends consideration of a parallel "virtualization overlay" approach, in which the Standards are revised such that the existing definitions and existing requirements are retained, but the proposed new definitions and new requirements are also an option. An entity must identify which approach they choose, on a cyber-system by cyber-system basis. This approach ensures backwards compatibility, minimizes the impact on entities that do not employ virtual technology, and yet frees other entities to pursue the possibilities of virtualization.

The overlay approach might by designed to sunset after a time, or be reassessed at a certain point based on lessons learned. It might be considered as a sort of CIP version of the PRC-005-2 to PRC-005-6 trransition.

Expansion of CIP scope to address new vulnerabilities associated with virtualization should be restricted only to virtualized BCS. These changes should not increase scope for non-virtualized BCS.

Seattle strongly urges that NERC sponsor a pilot project with volunteer utilities, as happened with CIP v5 changes be utilized with virtualization.

Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6	
Answer	
Document Name	
Comment	

Exelon appreciates the work and time that the SDT as put into this effort. We do see value in moving toward security objective-based requirements and being less technology dependent. We agree with many of the ideas, including splitting out lower risk monitoring from access control. However, we believe that the sweeping changings as now proposed are overly broad, including foundational definition changes, and these will radically impact current CIP programs.

As far as virtualization, Exelon has successfully implemented virtualization using a “conservative” architecture approach, while maintaining compliance with the current CIP requirements. We do see the potential of architecting virtualization and other technologies in new ways in the future to increase reliability and security while decreasing cost. CIP Standard changes to address new technologies and architectures are needed but are more appropriately addressed in a separate longer-term and comprehensive CIP version change effort. That effort should also take into consideration many other factors beyond virtualization that have surfaced since CIP V5 to improve the CIP Standards overall. Such an effort we could support.

We would prefer to see the current SDT address the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized environment using the existing body of standards, as currently approved.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA). We appreciate the work of the Standards Drafting Team in addressing the changing technology needs of industry.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI

Answer	
Document Name	

Comment

In general AECI agrees with the revisions to address virtualization for the follow reasons:

*Not materially changing non-virtualization compliance

* Providing the explicit ability to demonstrate compliance while using virtualization

* Allows CIP compliance program concepts to mature as the BCA term is retired

Additionally AECI raises an additional concern that the standards may not adequately address the “shared responsibility” aspect of using cloud computing resources, such as Azure or AWS. This was a topic of discussion at a recent NERC CIPC meeting, FedRAMP requirements were explained as possibly being a good model for addressing the shared responsibility issues. (https://www.fedramp.gov/)

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	
Document Name	

Comment

Thank you for the opportunity to comment

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	
Document Name	

Comment

We urge the drafting team to implement this in stages and consider the EACS/EAMS and PACS/PAMS changes initially. These changes will have the least operational impact and the greatest security benefits. Introduction of secured configuration and CIP-005 changes should be transitioned over time to reduce operational risk and impact.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"In the development of EEI comments, we have struggled with trying to find some middle ground that acknowledges the hard work and laudable efforts made by the SDT, unfortunately, the structure of the comment format did not lend itself to such comments. Additionally, while EEI's comments may be viewed as largely negative; we recognize that many of the ideas being developed by the SDT have significant future merit. Nevertheless, we cannot support the level of change being proffered at this time due to the recognition that virtualization remains a niche effort within the industry and will continue as such for the foreseeable future. This has led us to the conclusion that SDT efforts need to focus more on the how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption.

EEI does not support the overly broad and sweeping change proposed by the SDT because it is premature. While there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time would prove to be too disruptive to existing efforts by the industry. Furthermore, there is limited acceptance of virtualized networks within the industry and efforts to try and tailor the current body of standards to accommodate this emerging security solution is likely to create needless security concerns. Instead the SDT should work toward addressing the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized environment using the existing body of standards, as currently approved. We further believe that the level of change being considered by the SDT would be better addressed through a separate initiative spanning several years to allow more engagement by the industry.

EEI also notes that while the SDT has offered up some very interesting ideas to address virtualization within BES Cyber Systems, many Responsible Entities still feel there is a lack of overall clarity necessary to address the design, control, and protection of these systems in a virtualized environment.

EEI's last concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, we are concerned that from an audit perspective this approach may prove to be very difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effective and consistently audited."

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	
Document Name	

Comment

Be consistent with the use of "such as", "e.g.", and other illustrative phrases. While the changes proposed are a definite improvement to the standards, there will be a significant cost to implement these changes. These include revisions to change management systems, inventory systems, and other supporting tools used for audit evidence. As the drafting team looks at the implementation plan for these changes, consider how to allow entities to absorb these costs over time.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES

Answer	

Document Name	
Comment	
Overall, LES supports the direction of this project.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	
Comment	
SMEC appreciates the efforts of the SDT. However, we disagree with the approach of substantial changes to numerous standards and definitions in order to address virtualization. SMEC suggests that a better solution would be a new CIP standard that applies to virtualized CIP Systems or to provide clear implementation guidance on protecting BES Cyber Systems within virtualized environments under the existing framework and standards already in place. SMEC is concerned that this magnitude of change to the CIP standards when many entities have not yet been audited for CIP v5 would be too disruptive to non-virtualization compliance.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	
Document Name	
Comment	
NYPA is concerned given the proposed expansion of the Secure Configuration concept, as this has the potential to significantly increase the scope of identified BES Cyber System Information, thereby adding administrative overhead to track this, and the creation of numerous new BCSI documents / repositories which poses a risk.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	

Answer	
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
Support MRO NSRF additional comments	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP requests that SDT provides technical guidelines and examples for each requirement that has been modified/added.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	
Document Name	

Comment
LCRA would like to thank the drafting team for the time and effort invested in creating these proposed changes.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	
Document Name	

Comment
General overall comment, the newly proposed definitions need to be re-evaluated, clarified, and agreed before the standards and requirements can be fully understood.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	
Document Name	

Comment
In NPPD's opinion the proposed changes are too wide sweeping and transformational in nature without adequately addressing the more immediate need to clarify how the security and management of CIP systems in virtualized environments (or any new emerging technology) can be accomplished. Changes of this magnitude should be accomplished under a separate initiative with an adequate timeframe that allows proper engagement with industry to develop an approach to CIP compliance that can better adjust to changes in technology and risk environments. NPPD does encourage the drafting team to develop industry guidance for virtualization. However, as stated, the industry should have a focused (not rushed) effort to evaluate what is needed within the CIP Standards as changing or new technology emerge. Continual overhaul of the NERC Standards means increased risk to the Bulk Power System, as resources are siphoned off to align entity programs to continual change to the Standards. NPPD encourages the drafting team to issue guidance to the industry on virtualization and, if necessary, develop a single separate NERC Standard for Virtualization. However, a larger overall solution must be attained for new/emerging technologies and risk without the continual overhaul of the CIP suite of Standards

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	AZPS Comments - Question 16.docx
Comment	
Please see the attached document.	
Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
IESO agrees that the changes only needed to “backwards compatible” from a controls/ program perspective. IESO agrees that, as a primary consideration, the proposed changes do not have to be “backwards compatible” at the device level	
Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
MEC appreciates all the thoughtful hard work the SDT has put into this effort. That said, the changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.	

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	
Document Name	

Comment

Xcel Energy fully supports the comments submitted by the MRO NSRF and Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	
Document Name	

Comment

Moving to a security objective approach implies for a need for a cyber-security plan which considers the risk and appropriate mitigation and controls to meet the objective.

In the development of our comments, we have struggled with trying to find some middle ground that acknowledges the hard work and laudable efforts made by the SDT, unfortunately, the structure of the comment format did not lend itself to such comments. Additionally, while our comments may be viewed as largely negative; we recognize that many of the ideas being developed by the SDT have significant future merit. Nevertheless, we cannot support the level of change being proffered at this time due to the recognition that virtualization remains a niche effort within the industry and will continue as such for the foreseeable future. This has led us to the conclusion that SDT efforts need to focus more on the how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption.

We do not support the overly broad and sweeping change proposed by the SDT because it is premature. While there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time would prove to be too disruptive to existing efforts by the industry. Furthermore, there is limited acceptance of virtualized networks within the industry and efforts to try and tailor the current body of standards to accommodate this emerging security solution is likely to create needless security concerns. Instead the SDT should work toward addressing the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized

environment using the existing body of standards, as currently approved. We further believe that the level of change being considered by the SDT would be better addressed through a separate initiative spanning several years to allow more engagement by the industry.

We also note that while the SDT has offered up some very interesting ideas to address virtualization within BES Cyber Systems, many Responsible Entities still feel there is a lack of overall clarity necessary to address the design, control, and protection of these systems in a virtualized environment.

Our last concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, we are concerned that from an audit perspective this approach may prove to be very difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effective and consistently audited.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Each change to a standard creates additional work for an entity to evaluate its processes, revise where appropriate, implement the changes, and retrain employees, which is not cost-effective. The proposed changes to the CIP standards will have significant impacts on entities and will require substantial resources to implement. The proposed changes go beyond simply updating technology and/or documentation; they constitute a culture shift comparable to the CIP v5 transition. Entities must implement processes to achieve an understanding of new terms, buy in to their use, and change their the culture to employ new terms. Entities must be provided sufficient time to determine the effects of the revised requirements and definitions, develop adequate processes, and train personnel appropriately in order to implement quality practices that improve BES reliability. Reclamation recommends a minimum of 24 months for all entities to implement the proposed changes, with an additional 18 months for entities that use virtualization to achieve compliance.

Where possible, Reclamation recommends the SDT use the following existing industry terms:

Intrusion Detection and Prevention System (IDPS) – Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System(s) (IPS) – System(s) that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Intrusion Detection Systems (IDS) – System(s) that detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Enclave – A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Enclave Boundary – Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a wide area network (WAN).

Reclamation recommends adding the following new terms to the NERC Glossary of Terms:

Physical Access Control and Monitoring System (PACMS) – 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.

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	
Document Name	

Comment

Given that as long as the virtual CIP Cyber Assets are identified appropriately, most of existing CIP V5 requirements worked with these virtual CIP Cyber Assets very well based on previously NERC and MRO's advices regarding virtualization. We disagree with these significant directional changes that are only for sufficing a very small percentage of the virtual devices while ignoring the fact that the majority of physical devices are working smoothly for the existing requirements. The major issue for the existing CIP V5 requirements is that the virtual Cyber Assets are not explicitly required in the current standard language. After revising the Cyber Asset definition to include the virtual devices, most of the compliance issues will be resolved. SDT's strategy for the virtualization should focus on developing few additional requirements that only apply to the virtual CIP Cyber Assets if the existing requirements cannot be addressed in the virtual environment. Resulting from we suggested strategy, it would be beneficial for all registered entities as follows:

• For the registered entities that have no any virtual CIP Cyber Assets, they may not need to do anything.

• For the registered entities that have some virtual CIP Cyber Assets, they would only need to address the additional requirements for their virtual CIP Cyber Assets unless they could resolve them using the existing requirements.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory

Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

The MRO NSRF remains concerned with the subjectivity this will bring to meeting compliance. Auditors come from varying backgrounds and while one auditor may not have an issue with an entity's risk based assessment, the next auditor may. This may even be true with an entity. The industry experienced this with the CIP-002 RBAM and then was later asked to change to a more prescriptive set of requirements.

We do not agree with the SDT direction at this time. The NSRF feels that the proposed changes are too wide sweeping and transformational in nature without adequately addressing the more immediate need to clarify how the security and management of CIP systems in virtualized environments can be accomplished. Changes of this magnitude should be accomplished under a separate initiative with an adequate multi-year timeframe that allows proper engagement with industry to develop a new approach to CIP compliance that can better adjust to changes in technology and risk environments.

In the meantime, we recommend that the SDT narrow their focus back to the issue at hand which should be clarified standards and guidance for systems that exist within a virtualized environment. One possible recommendation would be to look at the development of a new CIP Standard that solely addresses the base level controls, security and configuration requirements for virtualized CIP systems and modify other existing CIP Standards and Requirements to exempt virtualized systems when applicable. Taking this approach would provide the clarity that is needed today for entities currently utilizing or planning to utilize virtualization with their CIP systems without requiring yet another complete NERC CIP program overhaul

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3,5

Answer	
Document Name	

Comment

AEP is concerned with the addition of veiled requirements to conduct “risk” analyses in proposed CIP-010-4 R3 Parts 3.5 and 3.6. Our understanding is that the “impact to the BES” is in fact the risk based on the equation used when the bright lines were established: Risk equals Threat times Vulverability times Impact, where Impact is the only variable and Threat and Vulnerability are defined as being equal to one. Also, sufficiency criteria for the risk analysis have not been established so this will likely become another source of contention when compliance is assessed. The work involved with assessing and documenting the “risk” for every component of every high and medium impact BCS across the BES will be enormous. AEP believes there should be an alternative to the “risk” analysis, stated in the Requirement, such as checking for patches and implementing/mitigating on the current 35 day cycles.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

PacifiCorp’s approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be addressed here.

PacifiCorp does not support the overly broad and sweeping change proposed by the SDT, feeling that the effort is premature. While there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time would prove to be too disruptive to existing efforts by the industry.

PacifiCorp’s primary concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, we are concerned that from an audit perspective this approach may prove to be very difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effective and consistently audited.

The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective.

It is not clear how the magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6

Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
It appears most of these changes are not specific to virtualization as the project indicates. Rather, the changes indicate a shift in the CIP Reliability Standards. As the industry recently implemented version 5 of the CIP standards, this puts an additional burden to comply with the proposed changes. Texas RE is not convinced a shift in the CIP standards is necessary. If the SDT feels it is necessary, the entire body of CIP Reliability Standards should be evaluated. Texas RE requests the SDT provide justification for the proposed changes by the V5 TAG, since that is what is referenced in the June 1, 2016 Standards Authorization Request.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	
Cowlitz supports APPA comment. Futher, we believe the standards must evolve to allow virtualization application.	
Likes 0	
Dislikes 0	

Response

Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	
Document Name	

Comment
PGE supports the direction that the drafting team is taking. The CIP standards framework should not serve to limit the use of new technologies that meet the security objectives and this poposed set of standards makes great strides in accomplishing that outcome. PGE encourages the continued engagement of FERC and the ERO enterprise to develop and document consistent approaches to implementing and auditing these new standards.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	
Document Name	

Comment
A concept not address in the concepts in a virtual TCA. So, in a virtualized environment if an entity spins up a new virtual machine, but the wrong base image was used, and it is deactivated within 30 days of creation is it now a TCA? The creation of virtual machines should be addressed. Is cloning from a base virtual machine in the environment acceptable since it already has all the security controls applied? What about when a new base image needs to be created? Must it be created in a test bed first then moved to production. However, typically the security controls of policies and targets for systems managing backups, anti-malware, logging and other may be different. So, can a new virtual machine have only some security controls in place if they are applied in a reasonable time frame when connected to production? This is also a problem for new physical equipment as well. As pointed out in another comment, some of the V5TAG items in the Standards Authorization Request are not addressed by these proposed revisions. We appreciate the SDT's effort on this issue. While our comments may appear negative, they are only pointing out the problems and concerns we have identified. The revisions to CIP-010 R1, R3, and CIP-007 R2 are a step in the right direction when it comes to the current pains of CIP compliance. If the SDT focused on those changes and the V5TAG issues remaining, then we might be able to get to a better set of requirements. However, some of the overly broad and sweeping changes to both defined terms and requirements may be more than the industry can digest at this time. The SDT needs to focus on how virtualization fits into the current requirements. Furthermore, we like the idea of meeting security objectives with a selection of one or more protection elements to achieve the objective. This is much better than overly prescriptive controls that do not always fit. We prefer examining this path and not the other fork in the road with overly prescriptive requirements trying to tie an industry to best practices as they exist today. If the SDT wanted to future proof the requirements then the requirements should be reworked with the stated security objective and let the Entity develop a program or plan to address that security objective and include the identification of the controls, and potentially a means to measure control effectiveness. An Entity would have to maintain an effectiveness greater than X to stay compliant. Or a third-party review like CIP-014 could be implemented. The threat remains relatively unchanged over the years; someone with malicious intent causing adverse impact to one or more BES Facilities. However, the attack vectors and protections against those attack vectors continue to change. Unless Entities can be allowed to develop their

own programs to identify the attach vectors and protections, then the requirements will always lag the existing threat landscape when new vectors are identified.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	
Document Name	
Comment	
Because the new standards would be moving away from a prescriptive approach into a more fluid one, CPS Energy will need to make sure we have in writing our reasoning behind our thresholds/our procedures in general. Our procedures will need to have this information for us to provide as evidence to the auditors. There should be another means for CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
In review, NRG asserts that the modifications presented by the SDT represent a drastic shift in philosophy of the standards that are significantly more substantial than an introduction of virtualuzation defintion, akin to the shift from v3 to v5. NRG applauds the SDT in the attempt at shifting the focus to enourage security. However, an ambiguous approach could lead to a wide disparity in implementation between Registered Entities. This could `make the auditing of CIP much more subjective and also industry inderstanding much more subjective also. The shift raises concerns of reintroducing difficulties from previous versions of the standards, i.e. risk-based methodology for CIP-002 and “spaghetti” requirements.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	

Document Name	
Comment	
Be consistent with the use of “such as,”, “e.g.,” and other illustrative phrases. While the changes proposed are a definite improvement to the standards, there will be a significant cost to implement these changes. These include revisions to change management systems, inventory systems, and other supporting tools used for audit evidence. As the drafting team looks at the implementation plan for these changes, consider how to allow entities to absorb these costs over time.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	
Document Name	
Comment	
Because the new standards would be moving away from a prescriptive approach into a more fluid one, CPS Energy will need to make sure we have in writing our reasoning behind our thresholds/our procedures in general. Our procedures will need to have this information for us to provide as evidence to the auditors. There should be another means for CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	
Document Name	

Comment

In the development of EEI comments, members struggled with trying to find some middle ground that acknowledges the hard work and laudable efforts made by the SDT as most members identified with the progressive, forward thinking of several proposed concepts. However, EEI members agree that many of the ideas being developed by the SDT have merit.

As noted in question 1, these comments do not represent a consensus, but we offer them for the SDT to consider. At this time, the EEI members who participated in the development of these comments do not support the level of change being proffered due to the recognition that virtualization remains limited in its adoption within the industry and is expected to continue as such for the foreseeable future. This is not to diminish the fact that in many sectors outside of the electric utility industry virtualization is making great advancements that enable many security improvements. EEI recognizes that the existing CIP reliability standards may be overly prescriptive and at times drive unnecessary costs, while limiting security benefits available through the application of modern technology. Nevertheless, fixing these problems needs to be taken a step at a time to avoid disruption to existing systems and processes used by companies. EEI encourages the SDT to focus more on how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption.

Given the pace of change of the CIP reliability standards to which the industry has been responsive and will continue to be responsive as it contemplates upcoming compliance effective dates, the members who participated in the development of these comments do not, at this time, support the overly broad and sweeping changes proposed by the SDT. For these members, the modifications are premature and, while there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time could prove to be too disruptive to existing efforts by the industry. Furthermore, the use of virtualized networks within the industry is still limited and efforts to try and tailor the current body of standards to accommodate this emerging security solution is likely to create new security concerns. Instead, we encourage the SDT to work toward addressing the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized environment using the existing body of standards, as currently approved. Additionally, EEI further suggests that the level of change being considered by the SDT may be better addressed through a separate initiative spanning several years to allow more engagement by the industry.

EEI also notes that, while the SDT has offered up some very interesting ideas to address virtualization within BES Cyber Systems, many Responsible Entities still feel there is a lack of overall clarity necessary to address the design, control, and protection of these systems in a virtualized environment.

EEI's last concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, there is concern that, from an audit perspective, this approach may prove to be difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effectively and consistently audited.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3

Answer	
Document Name	

Comment

Hydro One supports the comments submitted by NPCC TFIST. In addition, the real fork maybe it is time to determine whether the CIP set of Standards are ready to be transitioned into a full risk-based set of standards (starting from CIP-002) rather than control-based set of standards. The SDT is trying to have it both ways for the sake of backwards compatibility. In the current proposed revisions, certain security controls are maintained mainly for routable protocols and objective oriented requirements are being introduced to address virtualization. backwards compatibility is a desired outcome but it maybe time for SDT to consider the following:

- Is the industry mature enough for a full risk-based approach to cyber security?
- Have the auditors figured out how to audit CIP standards in a more risk-based/objective oriented world?

Until the answer to both questions above are “yes”, Hydro One recommends that the SDT develop one or more standard(s) with a set of controls applicable to virtualized components.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

LIZ – in conjunction with hardware separation makes sense, but by itself leaves a lot of opportunity for failure due to misconfiguration

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	
Document Name	

Comment

Regarding the definitions, please clarify how a virtual switch that is creating a LIZ should be categorized?

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Santee Cooper appreciates the SDTs effort in drafting the complex virtualization standards.

CIP-005 1.1-1.1.1. Are you talking about a firewall or something else to logically isolate our systems? How could this be accomplished when using dial up? Will dial-up require the use of an EAMS?

CIP-005 2.1 - With the revised definition of Intermediate System and Interactive Remote Access does this mean an Intermediate System is required to connect with medium impact sites that use dial up? CIP-005 2.2 – With the removal of "with External Routable Connectivity" under applicable systems, are dial up connections going to be required to be encrypted?

CIP-005 2.3 – With the removal of "with External Routable Connectivity" under applicable systems, will multi-factor authentication be required for dial up systems?

CIP-010 – This is a situation where in the past the prescriptive model would be a better fit than the higher level objective based model. Currently this standard is specific on what the expectations are and what needs to be done to meet the requirements of the standard. In the proposed revision requirements they are too vague and leave it open to an auditor's interpretation.

For entities not pursuing virtualization, these revisions tend to create more confusion around what is required for compliance.

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 no Dominion and NYPA

Answer	
Document Name	

Comment

Moving to a security objective approach implies for a need for a cyber-security plan which considers the risk and appropriate mitigation and controls to meet the objective.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	
Document Name	
Comment	

1. As written, the proposed changes in the standard package may add unintended compliance risk to applicable entities. The standard proposes flexibility to allow the responsible entity to implement controls for the Secure Configuration; however, this may not comport to audit situations where the auditors are deciding whether the entity's controls meets the auditors' expectations of compliance. The SSRG suggests anticipates the Implementation Guidance document to be posted in the future may relieve some of these concerns.

2. Questions to consider: How will the retirement of the defined term for EACMS affect the Order 848 FERC directed CIP-008 changes? Will CIP-008 need revising once this current project is approved by FERC? Should changes to CIP-008 be part of this exercise?

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	

Generally speaking, Southern Company is in favor of this change in methodology. These changes will facilitate the use of more current and potentially more secure technology while allowing Registered Entities the flexibility to use virtualized or physical systems to do so. We recognize the inherent risk in any change to the compliance methodology and wish to embark on such changes taking care to balance the risk associated with the change with the benefits received from the change.

That said, additional clarity and technical guidance is needed in documenting a Secure Configuration. Southern would like to see more clarity in how far the Secure Configuration boundary goes. At this time, it appears overly broad and we are concerned that it may start to include things like firewall rules, iDRACs and other more in-depth configuration items.

Likes 0	
Dislikes 0	
Response	

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	
Document Name	
Comment	

PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	
Comment	

APPA recognizes the complex and difficult job the SDT had in drafting the virtualization standards. The SDT's efforts are appreciated. Project 2016-02 provides best practices for security standards that strive to stay ahead of adversaries' efforts. The Project is groundbreaking and is the first step toward the next level of the best practices in security standards. APPA acknowledges that the comments herein largely question the draft standards and request clarity. Because the questions are open ended, public power did not see a need to provide yes/no answers, believing that is best left too registered entities. Public power sees this effort to date as significant progress.

Importantly, implementing the virtualization standards will be a challenge for NERC and industry. APPA, therefore, believes that the implementation plan and its timing is now the most crucial consideration. APPA encourages the SDT to draft an implementation plan with a two- to four-year implementation phase. The implementation plan needs to be facilitated by sufficient guidance. Guidance will need to be provided during implementation based on best practices learned during the implementation period. The period of putting Project 2016-02 in place should be a phase of learning so that best security practices can be implemented by all entities big and small. Because these changes are extensive, involve complex new concepts, and may have many unintended consequences, a pilot project involving volunteer utilities and NERC should be part of the implementation effort for these changes, similar to the pilot performed for the CIP v5 transition.

To reiterate, the following are some general principles that might be applied to guide revisions to the proposed virtualization changes:

1. APPA supports the SDTs efforts on proposed changes and believe this is a great initial step.

2. Changes are more extensive than expected, probably have many unintended consequences, are complex and largely untried, and in some cases expand CIP scope to address new vulnerabilities introduced by virtualization.

3. Therefore, consider a parallel "virtualization overlay" approach, in which the existing definitions and requirements are retained, but the proposed new definitions and new requirements are also an option. An entity must identify which approach they choose, on a cyber-system by cyber-system basis.

4. The overlay approach might sunset after a time or be reassessed at a certain point based on lessons learned.

5. Expansion of CIP scope to address new vulnerabilities associated with virtualization should be restricted only to virtualized BCS. These changes should not increase scope for non-virtualized BCS. 6. Public power strongly urges that a NERC-sponsored pilot project with volunteer utilities, as happened with CIP v5 changes, be utilized with virtualization.
Likes 0
Dislikes 0
Response