Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization - Draft 2
Comment Period Start Date:	6/30/2021
Comment Period End Date:	9/1/2021
Associated Ballots:	2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 AB 2 ST

There were 93 sets of responses, including comments from approximately 218 different people from approximately 137 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

2. The Applicable Systems column may include "SCI identified independently…" Is this clear or is additional clarification (such as "SCI identified as supporting, but not part of…") needed?

3. The SDT modified the ERC definition to reference "outside the asset containing". This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

4. The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

5. The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

6. The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

7. As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

8. The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

9. The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

10. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

11. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

12. The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

13. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

14. Please provide any additional comments for the SAR drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	Ali Miremadi	CAISO	2	WECC
					Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC

Eversource Energy	Christopher McKinnon	3		Eversource 1	Christopher McKinnon	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Portland General Electric Co.	Daniel Mason	6		PGE FCD	Ryan Olson	Portland General Electric Co.	5	WECC
					Nathaniel Clague	Portland General Electric Co.	1	WECC
					Angela Gaines	Portland General Electric Co.	3	WECC
					Daniel Mason	Portland General Electric	6	WECC
Snohomish County PUD No. 1	Holly Chaney	3		SNPD Voting Members	John Martinsen	Public Utility District No. 1 of Snohomish County	4	WECC
					John Liang	Snohomish County PUD No. 1	6	WECC
					Sam Nietfeld	Public Utility District No. 1 of Snohomish County	5	WECC
					Alyssia Rhoads	Public Utility District No. 1 of Snohomish County	1	WECC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC

					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power, Inc.	1	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	4	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Jodi Jensen	Western Area Power Administration - Upper Great Plains East (WAPA)	1,6	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO

					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1,3,5	MRO
					Joe DePoorter	Madison Gas and Electric	4	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					Bill Shultz	Southern Company Generation	5	MRO
Southwest Power Pool, Inc. (RTO)	Kimberly Van Brimer	2	MRO,WECC	Southwest Power Pool Standards Review Group (SSRG)	Kim Van Brimer	SPP	2	MRO
					Jim Williams	SPP	2	MRO
					Matt Harward	SPP	2	MRO
					Shannon Mickens	SPP	2	MRO
					Alan Wahlstrom	SPP	2	MRO

FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		CHPD	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company -	5	SERC

						Southern Company Services, Inc. - Gen		
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC

Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
Nurul Abser	NB Power Corporation	1	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
Vijay Puran	NYSPS	6	NPCC
ALAN ADAMSON	New York State Reliability Council	10	NPCC
Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
Brian Robinson	Utility Services	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Jim Grant	NYISO	2	NPCC
John Pearson	ISONE	2	NPCC
Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
Chantal Mazza	Hydro-Quebec	2	NPCC
Michele Tondalo	United Illuminating Co.	1	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC

					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Scott Miller	Scott Miller		SERC	MEAG Power	Roger Brand	MEAG Power	3	SERC
					David Weekley	MEAG Power	1	SERC
					Steven Grego	MEAG Power	5	SERC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	6	SPP RE	OKGE	Sing Tay	OGE Energy - Oklahoma	6	MRO
					Terri Pyle	OGE Energy - Oklahoma Gas and Electric Co.	1	MRO
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
		5			Michael Shaw	LCRA	6	Texas RE

Lower Colorado River Authority	Teresa Krabe			LCRA Compliance	Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Associated Electric Cooperative, Inc.	Todd Bennett	3		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
					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
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					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. Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

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

Answer	No
Document Name	

Comment

The proposed definition of CIP System is confusing. Dominion Energy recommends removing CIP System from the proposed defined terms and all references to the CIP System defined term throughout the definitions. Dominion Energy recommends addressing the issues of applicability it appears the CIP System definition was intending to do at the Standard level.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

It is understood that when SCI is included in the CIP Systems it is to be treated like the CIP System. However, the other option for identification of SCI is not clear, as discussed in greater detail in the response to question 2.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

It is understood that when SCI is included in the CIP Systems it is to be treated like the CIP System. However, the other option for identification of SCI is not clear, as discussed in greater detail in the response to question 2.

Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Consider modification of SCI to be based on the Cyber Asset definition. SCI's basis on the "programmable electronic devices" terminology makes it unclear as to what type of devices are the intended target of the standard. CIP-002 provides guidance for identification and classification of BCS (grouping of BCAs). Other associated cyber assets are classified based on their connectivity, protection and relationship to the BCAs. Suggest remove SCI identification from CIP-002.	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	
Comment	
The current definitions and requirement language place BCS, which are groups of Cyber Assets, at the same level as SCI. SCI is likely to be handled as individual devices. This adds complexity both to the CIP-002 R1 compliance process as well as creates complexity for CIP-002 R2.2 approval processes. Duke Energy requests that the SDT add a definition and update requirements to leverage the concept of an SCI Group (SCIG). This would establish parity between the BCA -> BCS relationship with SCI -> SCIG. This also further simplifies applicability in the downstream standards from the current "High Impact BES Cyber Systems (BCS) and their associated: EACMS; PACS; and PCA" with a separate line for "SCI identified independently supporting an Applicable System above" to "High Impact BES Cyber Systems (BCS) and their associated: EACMS; PACS; PCA; and SCIG". Further, the CIP-002 language can now be simplified to the following, which retains closer parity with current language while still addressing the SDT's intentions: "Identify each of the high impact BES Cyber Systems, if any, and associated Shared Cyber Infrastructure Groups, if any, according to Attachment 1, Section 1 at each asset".	
Likes 0	
Dislikes 0	
Response	

Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
We believe the options are mostly clear and acceptable with the exception of the phrase “independent SCI supporting” either high or medium impact. It is unclear and confusing how an SCI can be both independent and supporting simultaneously. The proposed revised definition of BES Cyber System already would make it clear that SCI is to be included in CIP scope if applicable. We recommend removing the second bullet point entirely from both R1.1 and R1.2.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
The identification of SCI is not clear within CIP-002, nor is it understood that SCI should be high-water marked to the highest impact applicable system that is sharing its infrastructure. The only thing that makes this clear is the definition of CIP System, which term is not used within CIP-002.	
Likes 0	
Dislikes 0	
Response	

William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
The identification of SCI included in a CIP System is clear but the identification of Management Systems included in SCI is unclear. For the all-in scenario, with Provider1 as an example, the Provider management Cyber Asset would typically be outside the ESP currently. With the new all-in, that CA would be a Management Interface, and would then be included as part of the SCI per the SCI 'including Management Interfaces' definition, which would then pull the CA into the BCS, making it a BCA, so it can no longer be outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
It is confusing to understand the definition of Shared Cyber Infrastrure (SCI) and therefore the overall requirement is unclear. While significant education to industry would improve this, it is extremely dependent on interpretation by stakeholders and auditors.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
The CIP-002 should maintain a section on BROS that establish the relationship with the BCS	
Likes 0	
Dislikes 0	
Response	

Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
We believe the options are mostly clear and acceptable with the exception of the phrase “independent SCI supporting” either high or medium impact. It is unclear and confusing how an SCI can be both independent and supporting simultaneously. The proposed revised definition of BES Cyber System already would make it clear that SCI is to be included in CIP scope if applicable. We recommend removing the second bullet point entirely from both R1.1 and R1.2. On a related note, we are concerned about revising the existing CIP standards to address virtual technologies and believe a better approach may be to address the majority of impacts and new requirements in a new standard. Please see our comment on this in response to question #14.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The term 'SCI' is still unclear and ambiguous.The term 'SCI' is still unclear and ambiguous.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA supports the “All-In” option which identifies the SCI is to receive the impact rating based on the BCS that it hosts. It is not clear how the identified independently option is to be evaluated.	
Likes 0	

Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	

Comment
It is not clear what is meant by independent SCI supporting any part of the high impact BCS.

Likes 0	
Dislikes 0	

Response

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

Comment
Texas RE does not agree that the two options for identification of SCI are clear. The distinction between SCI included in a BES Cyber System (BCS) and SCI operating independently adds an unnecessary level of complexity to the standards. Texas RE recommends there be only one option, which is to categorize SCI as meeting the definitions of the VCAs they are hosting and subsequently include the SCI within BCS, Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) and Protected Cyber Assets (PCAs), as applicable. Additionally, Texas RE recommends that registered entities be required to identify all BCS, as well as their associated EACMS, PACS, and PCAs, as applicable. System (PM5) and system component (CM-8) inventory are both controls from NIST 800-53 Rev. 5. Texas RE is concerned CIP-002-7 would be less effective if registered entities are not required to implement the full suite of the system and component inventory protections in a manner consistent with these requirements.

Likes 0	
Dislikes 0	

Response

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

We support NPCC TFIST's comments as found below:

Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact?

Request clarification of “it is a part of for CIP Requirement Applicability?” Is there a missing word? Should the language be “it is a part of it for CIP Requirement Applicability?”

Request clarification of the or in 1.3. Is the entity identifying low impact BCS or supporting SCI or both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

The standard is clear about the two options. However, the Technical Rationale it is not clearly understood how the Standards Drafting Team anticipates treatment of systems.

Likes 0	
Dislikes 0	
Response	

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	

In support of NPCC RSC comments.

Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact?

Request clarification of “it is a part of for CIP Requirement Applicability?” Is there a missing word? Should the language be “it is a part of it for CIP Requirement Applicability?”

Request clarification of the or in 1.3. Is the entity identifying low impact BCS or supporting SCI or both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?

We don’t understand how to categorize a Shared Cyber Infrastructure. The SDT seems to make a distinction between two types of SCI, one type is supporting, and the other type is independent supporting. Our hypothesis is that a “supporting SCI” is for BCS (BCA/PCA) and that an “independent supporting SCI” is for associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS)).

In both cases, the SCI is the categorization labels, like BCA, PCA, EACMS, PACS, TCA.

Yet in the Applicable Systems column in the other CIPs, the SDT seem to make a distinction between the SCI, for example

CIP-005 R1.5 1.5 … PACS hosted on SCI … SCI identified independently…

CIP-007 R1.1 SCI identified independently supporting.

Clarification is needed.

Are the two options for identification SCI required? Is there a difference in the controls that we want to apply?

We suggest simplifying the language or add more precision. Example:

Per Attachment 1, Section 1, identify each high impact BES Cyber System as either of the following, if any, at each asset; High Impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs) or SCI.

Furthermore, in the definition of SCI the PCA is not listed. Is this intentional? Wouldn’t be possible to have a PCA supported by an SCI? We suggest that the SDT review the SCI / VCA/ PCA definitions, adjust the applicability and the requirements.

Reference SCI: One or more programmable electronic devices, including the software and Management Interfaces, that share: • CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

While AEP agrees with the inclusion of this CIP-002 mechanism (the term CIP Systems) for including the associated applicable systems (EACMS, PACS, and PCAs) as a means to have a singular requirement for the identification of EACMS, PACS and PCAs, the current language appears to limit the identification of only those virtual systems (and underlying infrastructure) related to EACMS, PACS and PCAs. We believe this leaves a gap for the identification of those physical systems performing the same function(s). We recommend SDT to add clarifying language to allow for the identification of both physical and virtual systems as EACMS, PACS and PCAs under CIP-002.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

IESO supports the comments submitted to all the questions by both NPCC and ISO/RTO Council

Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact?

Request clarification of “it is a part of for CIP Requirement Applicability?” Is there a missing word? Should the language be “it is a part of it for CIP Requirement Applicability?”

Request clarification of the or in 1.3. Is the entity identifying low impact BCS or supporting SCI or both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?

We don’t understand how to categorize a Shared Cyber Infrastructure. The SDT seems to make a distinction between two types of SCI, one type is supporting, and the other type is independent supporting. Our hypothesis is that a “supporting SCI” is for BCS (BCA/PCA) and that an “independent supporting SCI” is for associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS)).

In both cases, the SCI is the categorization labels, like BCA, PCA, EACMS, PACS, TCA.

Yet in the Applicable Systems column in the other CIPs, the SDT seem to make a distinction between the SCI, for example

CIP-005 R1.5 1.5 … PACS hosted on SCI … SCI identified independently…

CIP-007 R1.1 SCI identified independently supporting.

Clarification is needed.

Are the two options for identification SCI required? Is there a difference in the controls that we want to apply?

We suggest simplifying the language or add more precision. Example:

Per Attachment 1, Section 1, identify each high impact BES Cyber System as either of the following, if any, at each asset; High Impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs) or SCI.

Furthermore, in the definition of SCI the PCA is not listed. Is this intentional? Wouldn't be possible to have a PCA supported by an SCI? We suggest that the SDT review the SCI / VCA/ PCA definitions, adjust the applicability and the requirements.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	Independently Identified SCI.jpg

Comment

The phrases "supporting SCI" and "independent SCI supporting" are not clear and should be removed from CIP-002. Resulting from SCI definition, SCI should be either a CIP cyber asset or no-CIP cyber asset, therefore SCI shouldn't appear in CIP-002 and Applicable Systems of CIP-003 to CIP-013. SCI should be used for identifying additional BCAs, EACMS, PACS or PCAs that could be missed in the virtualization environment.

For the proposed All-in-Scenario, SCI should be identified as a BCA, EACMS, PACS or PCA rather than a new classification of CIP cyber asset. For example, if a SCI can initialize, deploy and configure a BCA, it should be categorized as a BCA since it can remove a virtual BCA thus having an impact to the BES within 15 minutes. Similarly, if a SCI can initialize, deploy and configure an EACMS, it should be categorized as an EACMS since it can remove the virtual EACMS thus having electronic control function.

For independently Identified SCI as SDT proposed below, for the right side SCI, if the right SCI containing Management Interface can initialize, deploy and configure a CIP Cyber Asset, it should be categorized as a CIP cyber asset (See our comments above). If the right-side SCI hosts VCA that is a CIP cyber asset regardless of the impact rating, the right side SCI should be identified as the same impact CIP cyber asset it hosts. The right side SCI is out of CIP scope only: (1) if all VCAs it hosts are non-CIP cyber assets, this SCI would be out of CIP scope thus no need to be identified; (2) If it is used only to configure high impact network policy, it would be out of CIP scope since out of band management for CIP cyber assets is not required by the current CIP requirements scope and the SAR

Based on our comments above, the "SCI" and "independently Identified SCI" are not needed to be identified in CIP-002 since the SCI or independently Identified SCI either is a CIP cyber asset or out of CIP scope.

SEE ATTACHED DOCUMENT FOR PHOTO.

Resulting from our comments above, we recommend revising definitions of BCA, EACMS, PACS and PCA to include SCI so SCI would not be identified as another independently applicable CIP cyber asset. Our proposed changes align with FERC and NERC's security objectives and the SDT's goal to address cyber security risks to the reliability of the BES from virtualization technologies, while having less impact on the entities existing CIP programs, processes and documentation. Entities can use their existing CIP cyber asset identification processes to identify BCAs, EACMS, PACS and PCAs based on SCI and Management Interface language to address virtualization. If the responsible entities don't have virtualization, they wouldn't need to identify any additional CIP cyber assets at all.

Recommendations:

1. Restore the CIP-002 R1 and its Parts resulting from our proposed definitions changes below.

2. We propose the following changes to the new or existing definitions:

SCI:

SDT Proposed SCI definition

One or more programmable electronic devices, including the software and Management Interfaces, that share:

· CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or

· storage resources with any part of a BES Cyber System or their associated EACMS or PACS.

Each SCI is either:

· included in one or more BES Cyber Systems, EACMS, or PACS; or

· identified independently.

SCI does not include the supported VCA or CA with which it shares its resources.

NSRF Proposed Changes to the Definition

One or more programmable electronic devices, including the software and Management Interfaces in those devices, that share:

- CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, PACS or PCA; or
- storage resources with any part of a BES Cyber System or their associated EACMS, PACS or PCA.

This includes devices that contain Management Interfaces for virtualization management.

SCI does not include the supported VCA or CA with which it shares its resources.

Rationale: In the SDT proposed SCI definition, the device containing Management Interface is left out and is not identified as a CIP cyber part of SCI even though the management interface is in scope. For example, vCenter containing Management Interface, but it is not identified as a CIP cyber asset and is not protected. Also, PCA is missing from the SCI definition. In our proposed changes, it is not necessary to identify SCI independently since SCI would be identified as one of CIP Cyber Assets.

Management Interface:

SDT Proposed SCI definition

A user interface, logical interface, or dedicated physical port that is used to:

· Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or

· Provide lights-out management capabilities; or

· Configure an Electronic Security Perimeter;

excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Our Proposed Changes to the Definition

A user interface, logical interface, or dedicated physical port that is used to:

· Initialize, deploy, and configure BCA, EACMS, PACS, or PCA; or

· Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or

· Configure EAP of an Electronic Security Perimeter; or

· Configure EACMS that controls all communications to and from the BCS unless ESP model is used.

excluding physical user interfaces (e.g., power switch, touch panel, etc.). (See our rationale in Q6).

Rationale: In our view, the definition should focus on “in scope” CIP management interfaces. The term “Provide lights-out management capabilities” is not clear and should be removed since this criterion itself cannot make a management interface fall within CIP scope.

Also, the Management Interface on the SCI is absent. We have added a bullet in our proposed definition to address it.

Furthermore, we suggest edits to include:

a) changing configure an ESP to configure an EAP

b) adding configure EACMS to address the zero-trust mode based on our comments in Q4.

BCA:

SDT Proposed SCI definition

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded , or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Our Proposed Changes to the Definition

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or othe rwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. This includes SCI that is used for initializing, deploying and configuring BCAs or storing information for the real-time operation of BCAs.

Rationale: In our view, if a SCI meets BCA criteria, it must be identified as a BCA.

EACMS:

SDT Proposed SCI definition

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems and SCI grouped, by the Responsible Entity, in the EACMS it supports.

Our Proposed Changes to the Definition

Cyber Assets or Virtual Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems and SCI that is used for initializing, deploying and configuring EACMS or storing information for the real-time operation of EACMS.

Rationale: A SCI supporting EACMS doesn't make it to be part of EACMS. For instance, if a SCI only stores historical information for EACMS, it could be a BCSI repository rather than part of EACMS. In our view, only a SCI that can initialize, deploy and configure EACMS should be identified as EACMS.

PACS:

SDT Proposed SCI definition

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) (including SCI grouped, by the Responsible Entity, in the Physical Access Control Systems it supports) 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.

Our Proposed Changes to the Definition

Cyber Assets or Virtual 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. This includes SCI that is used for initializing, deploying and configuring PACS or storing information for the real-time operation of PACS.

Rationale: A SCI supporting PACS doesn't make it to be part of PACS. For instance, if a SCI only stores historical information for PACS, it could be a BCSI repository rather than part of PACS. In our view, only a SCI that can initialize, deploy and configure PACS should be identified as PACS.

PCA:

SDT Proposed SCI definition

One or more Cyber Assets or Virtual Cyber Assets that:

- Are within an Electronic Security Perimeter but are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or
- Share CPU or memory with any part of a BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to the Electronic Security Perimeter.

Our Proposed Changes to the Definition

One or more Cyber Assets or Virtual Cyber Assets that:

- Are within an Electronic Security Perimeter but are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or
- Share CPU or memory with any part of a BES Cyber System, EACMS, PACS or PCA; or

This includes SCI that is used for initializing, deploying and configuring PCA or storing information for the real-time operation of PCA.

Rationale: In the SDT proposed PCA definition, if the bullet 2 is for identifying PCA that shares resources with BCS, the ESP should be irrelevant. Also, it is not clear what the remediation actions are and why the one-time remediation makes it out of scope, noting that the compliance is an ongoing basis and the remediation shouldn't exclude a VCA from CIP scope. Furthermore, if SDT intends to protect non-CIP cyber assets that share the CPU or memory with CIP cyber assets, EACMS, PACS and PCA sharing resources with non-CIP cyber assets should also be considered rather than only BCS.

CA: Restore the CA definition.

Rationale: Given that SCI is defined as a programmable device, it meets the CA definition and should be treated as one type of CAs rather than excluding it from CA definition.

VCA: A logical instance of an operating system or firmware including software, data and virtual hardware on the logical instance hosted on a physical Cyber Asset.

BCS: Restore BCS definition.

Rationale: BCS should only include BCAs not other CIP cyber assets. Given that SCI could be an EACM, PACS or PCR, it shouldn't be included in BCS definition.

CIP System: This definition is not needed based on our proposed changes above.

Rationale: CIP System won't work for the CIP requirements since not each requirement applies to all CIP cyber assets that are included in the CIP System and the requirement has to specified which CIP cyber asset would apply.

ERC: Restore ERC definition since it is still effective (see our rationale in Q3).

EAP: Restore the definition

Rationale: Given that the current EAP is still clear and doesn't exclude policy-based rules, there is no need to modify EAP definition.

ESP: Restore ESP definition since it is still effective for the perimeter-based network protection (see the rationale in Q4).

IRA:

SDT Proposed SCI definition

User-initiated real-time access by a person from outside of the Responsible Entity's Electronic Security Perimeters (ESP) using a routable protocol:

· to a Cyber System within an ESP;

· through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;

· To Management Interfaces of Shared Cyber Infrastructure; or

· To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforces an ESP.

Our Proposed Changes to the Definition

User-initiated interactive access by a person employing a remote access client or other remote access technology using a routable protocol. (This includes cases where a routable protocol is converted to a non-routable protocol)

Remote access originates from a Cyber Asset or Virtual Cyber Asset that is:

a. not an Intermediate System

b. is not located within any of the Responsible Entity's Electronic Security Perimeter(s) or,

c. at a defined Electronic Access Point (EAP).

Interactive remote access does not include system-to-system process communications. (See our rationale in Q5).

Rationale: IRA definition should only define what remote access constitutes an IRA and shouldn't include the accessed end devices. The IRA accessed cyber assets should be addressed in the requirements rather than in the IRA definition. We propose to add additional language to clarify the routable protocol converting to non-routable still falls within IRA definition since the current IRA definition is not clear on this. The current IRA definition states the user-initiated access using a routable protocol and doesn't say all communication sessions need to be routable.

Intermediate System: Restore the IS definition since the current definition is clear and no need to redefine it.

Rationale: The proposed IS definition starts from "EACMS", which is not correct logically. A Cyber Asset should meet the IS definition and then becomes an EACMS. Otherwise an IS can be missed if it is not an EACMS originally.

BCSI: Restore the definition based on our proposed definition changes above.

Cyber Security Incident: Restore the definition based on our proposed definition changes above.

PSP: Restore the definition based on our proposed definition changes above.

Removable Medium: Restore the definition based on our proposed definition changes above.

Reportable Cyber Security Incident: Restore the definition based on our proposed definition changes above.

TCA: Restore the definition based on our proposed definition changes above.

We believe the options are mostly clear and acceptable with the exception of the phrase "independent SCI supporting" either high or medium impact. It is unclear and confusing how an SCI can be both independent and supporting simultaneously. The proposed revised definition of BES Cyber System already would make it clear that SCI is to be included in CIP scope if applicable. We recommend removing the second bullet point entirely from both R1.1 and R1.2.

Likes 0	
Dislikes 0	

Response

Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5

Answer	No
Document Name	

Comment

Recommend spelling out "Shared Cyber Infrastructure" and its acronym within the standard text.

Recommend including the definition within the text, or make a statement in the text directing to the definition in the definition list.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
The options for SCI association within CIP-002 may be clear, but the handling of SCI involving EACMS cases is not clear from CIP-002 since that standard is limited to assessment of HIGH, MEDIUM and LOW impact BCS cases.	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 3	
Answer	No
Document Name	
Comment	
GRE agrees with the comments submitted by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
In support of IRC SRC/SWG. Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact? Request clarification of “it is a part of for CIP Requirement Applicability?” Is there a missing word? Should the language be “it is a part of it for CIP Requirement Applicability?” Request clarification of the OR in 1.3. Is the entity identifying low impact BCS OR supporting SCI OR both?	

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Independent SCI supporting and supporting SCI are not clear. They should be removed from CIP-002.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The only exception of the phrase “independent SCI supporting” either high or medium Impact. The statement is unclear and confusing how an SCI can be both indendent and supporting sitmultaneously. The proposed revised definition of the BES Cyber System already would make it clear that SCI is to be included in CIP scope if applicable, It is recommended removing the second bullet entirely from both R1.1 and R1.2.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

We thank the SDT for it's work but believe the changes to definitions will create greatly impact existing entity's policies, procedures and documentation and increase administrative overhead when some basic changes can be drafted which will a) retain and address the issue of virtualization, b) allow entity's the flexibility to identify risks and implement appropriate security controls, and c) clarify language for regulators and industry alike. The current drafts create much administrative overhead because it requires entity's using virtual platforms to parse out subcomponents and assign risk to establish compliance for such components. As entity's move to cloud environments this will not be possible and therefore it is more practical to allow entity's to identify their systems, assess risk and categorize them based on hardware profiles. SCI does little to clarify and define. In general, WAPA recommends a focus on individual hardware components and software enforcment policies (AAA). For example, an entity could consider an ESXi platform a single BCS (or BCA) which contains VCAs. Just a perspective.

The phrases "supporting SCI" and "independent SCI supporting" are not clear and should be removed from CIP-002. Recommend that SCI should be either categorized as a CIP Cyber Asset or not a CIP Cyber Asset (Hardware based decision). SCI shouldn't appear in CIP-002 and Applicable Systems of CIP-003 to CIP-013. SCI should be evaluated using the criteria of a BCAs, EACMS, PACS or PCAs which can be missed in the virtualization environment.

For the proposed All-in-Scenario, SCI should be identified based on hardware such as BCA, EACMS, PACS or PCA rather than a new classification of CIP cyber asset. Creating separate definitions for SCI is tantamount to identifying hard drives and PCI cards as separate BCA and this will require entity's a great deal of administrative overhead.

Secondly, SCI that can initialize, deploy and configure a BCA should be categorized as a BCA since it has a high risk profile - can remove a virtual BCA and impact to the BES within 15 minutes. Similarly, if a SCI can initialize, deploy and configure an EACMS and should be categorized as an EACMS since it can remove the virtual EACMS and it's functions.

For independently Identified SCI proposed in the right box diagram below, SCI with an active Management Interface can initialize, deploy and configure a CIP Cyber Asset. This further supports the case for categorization based on hardware and not sub-components.

If the right-side SCI hosts VCA such as a CIP cyber asset regardless of the impact rating, the right side SCI should be identified as the same impact CIP cyber asset it hosts. It has the capability to impact the BES in 15 minutes. The right side SCI is out of CIP scope only: (1) if all VCAs it hosts are non-CIP cyber assets, this SCI would be out of CIP scope thus no need to be identified; (2) If it is used only to configure high impact network policy, it would be out of CIP scope since out of band management for CIP cyber assets is not required by the current CIP requirements scope and the SAR

Based on our comments above, the "SCI" and "independently Identified SCI" are not needed to be identified in CIP-002 since the SCI or independently Identified SCI either is a CIP BES Cyber Asset or not in scope.

We recommend revising definitions of BCA, EACMS, PACS and PCA to include SCI. Our proposed changes align with FERC and NERC's security objectives and the SDT's goal to address cyber security risks to the reliability of the BES from virtualization technologies, while having less impact on the entities existing CIP programs, processes and documentation. Entities can use their existing CIP cyber asset identification processes to identify BCAs, EACMS, PACS and PCAs based on SCI and Management Interface language to address virtualization. If the responsible entities don't have virtualization, they wouldn't need to identify any additional CIP cyber assets at all.

Recommendations:

1. Restore the CIP-002 R1 and its Parts resulting from our proposed definitions changes below.
2. We propose the following changes to the new or existing definitions:

SCI: One or more programmable electronic devices, including the software and Management Interfaces in those devices, that share:

- CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, PACS or PCA; or
- storage resources with any part of a BES Cyber System or their associated EACMS, PACS or PCA.

- Includes devices that contain Management Interfaces for virtualization management.
- SCI does not include the supported VCA or CA with which it shares its resources.

Basis for this Recommendation: PCA is missing from the SCI definition. In our proposed changes, it is not necessary to identify SCI independently since SCI would be identified as a CIP Cyber Asset(s).

Management Interface: A user interface, logical interface, or dedicated physical port that is used to:

- Initialize, deploy, and configure BCA, EACMS, PACS, or PCA; or
- Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or
- Configure EAP of an Electronic Security Perimeter; or
- Configure EACMS that controls all communications to and from the BCS unless ESP model is used.
- Excludes physical user interfaces (e.g., power switch, touch panel, etc.). (Refer to Q6).

Basis for this Recommendation: the definition should focus on “in scope” CIP management interfaces. The term “Provide lights-out management capabilities” is not clear and should be removed since this criterion itself cannot make a management interface fall within CIP scope.

- Also, the Management Interface on the SCI is absent. We have added a bullet in our proposed definition to address it.
- Furthermore, we suggest edits to include:
- a) changing configure an ESP to configure an EAP
- b) adding configure EACMS to address the zero-trust mode based on our comments in Q4

CA: Restore the CA definition.

Basis of this Recommendation: If SCI is defined as a programmable device, it meets the definition of a CA and should be treated as one type of CA’s rather than excluding it from CA definition.

VCA: A logical instance of an operating system or firmware including software, data and virtual hardware on the logical instance hosted on a physical Cyber Asset.

BCS: Restore BCS definition.

Basis of this Recommendation: BCS should only include BCAs not other CIP cyber assets. Given that SCI could be an EACM, PACS or PCR, it shouldn’t be included in BCS definition.

CIP System: This definition is not needed based on our proposed changes above.

Basis of this Recommendation: CIP System won't work for the CIP requirements since not each requirement applies to all CIP cyber assets that are included in the CIP System and the requirement has to specified which CIP cyber asset would apply.

ERC: Restore ERC definition since it is still effective (see our rationale in Q3).

EAP: Restore the definition

Rationale: Given that the current EAP is still clear and doesn't exclude policy-based rules, there is no need to modify EAP definition.

ESP: Restore ESP definition since it is still effective for the perimeter-based network protection (see the rationale in Q4).

IRA: User-initiated interactive access by a person employing a remote access client or other remote access technology using a routable protocol. (This includes cases where a routable protocol is converted to a non-routable protocol)

Remote access originates from a Cyber Asset or Virtual Cyber Asset that is:

3. not an Intermediate System
4. is not located within any of the Responsible Entity's Electronic Security Perimeter(s) or,
5. at a defined Electronic Access Point (EAP).

- Interactive remote access does not include system-to-system process communications. (See our rationale in Q5).

Basis for this Recommendation: IRA definition should only define what remote access constitutes as IRA and shouldn't include the accessed end devices. IRA accessed Cyber Assets should be addressed in the requirements rather than in the IRA definition. Recommend additional language to clarify the routable protocol converting to non-routable that falls within IRA definition - since the current IRA definition is not clear on this anyway. The current IRA definition states the user-initiated access using a routable protocol and doesn't refer to communication sessions needing to be routable.

Intermediate System: Restore the IS definition since the current definition is clear and no need to redefine it.

Basis for this Recommendation: The proposed IS definition starts from "EACMS", which is not correct logically. A Cyber Asset should meet the IS definition and then becomes an EACMS. Otherwise an IS can be missed if it is not an EACMS originally.

BCSI: Restore the definition based on our proposed definition changes above.

Cyber Security Incident: Restore the definition based on our proposed definition changes above.

PSP: Restore the definition based on our proposed definition changes above.

Removable Medium: Restore the definition based on our proposed definition changes above.

Reportable Cyber Security Incident: Restore the definition based on our proposed definition changes above.

TCA: Restore the definition based on our proposed definition changes above.

Likes 0	
Dislikes 0	

Response
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6
Answer	No
Document Name	
Comment
Please clarify if the SCI “form” as an Cyber System that includes the Management Interface will not require a separate Cyber Asset in the BCS List for the Management Interface provided the SCI Management Interface is the document IP address in CIP-007 R1.
Likes 0	
Dislikes 0	
Response
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan
Answer	No
Document Name	
Comment
OPG concurs with NPCC's RSC comments
Likes 0	
Dislikes 0	
Response
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1
Answer	No
Document Name	
Comment
Eversource recommends using "Independently identified". The term seems inconsistent in regards to how its used in all the CIP Standards.
Likes 0	
Dislikes 0	
Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT supports the IRC SRC comments and offers these additional comments:

- R1.1, bullet 1: Under the current version of CIP-002, there is no specific requirement to identify specific types of Cyber Assets applicable to the remaining CIP standards; it is implied at best. Going beyond the BCS identification into identifying specific Cyber Asset types, like Shared Cyber Infrastructure, is a change in to the fundamentals of CIP-002 and takes us back to CIP v1-v4 and the very granular level of Cyber Asset identification. The SDT should determine if all Cyber Asset types should be identified in CIP-002 or not. Each Cyber Asset type under the CIP standards is important in its role, including the SCI. If the SDT does not think that all Cyber Asset types should be addressed, SCI should be removed from this standard.
- R1.1, bullet 2: Please clarify the use of “independent.” It is unclear what this means. Independent of what?
- ERCOT recommends that no changes be made to requirement R1 in CIP-002.

Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	

While the expectation is clear with regard to what needs to be protected and why, what is not clear is what is required to achieve compliance with CIP-002 R1.1 requirements.

The requirement requires the identification of BCS as either “including any supporting SCI as part of the BCS” or with “independent SCI supporting any part of the high impact BCS or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).” This does not allow for the identification of BCS independent of having SCI, and therefore doesn’t account for non-virtualized environments.

The requirements and measures of CIP-002 do not sufficiently detail what is required to demonstrate compliance. The requirements are to create a list that identifies “each [BCS] as either” including supporting SCI or having independent SCI. However, the independent SCI details an association to EACMS, PACS, PCA. The requirement expects an identification of “BES Cyber Systems” but the sub-bullets imply an expectation to identify SCI and corresponding asset/system classifications. The measures and technical rationale provide no additional clarity other than creating lists. Is the expectation to simply provide identification that the identified BCS either include SCI or are supported by SCI (e.g. Yes/No or Checkbox), or is the expectation to explicitly identify and categorize SCI that meet this criteria (e.g. “1.) ABC High Impact BCS; 2.) CDE High Impact EACMS SCI”). If the expectation is to classify SCI, what should be the approach for classifying SCI that supports multiple classifications (e.g. EACMS and PACS)?

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	

Response

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact?

Request clarification of “it is a part of for CIP Requirement Applicability?” Is there a missing word? Should the language be “it is a part of it for CIP Requirement Applicability?”

Request clarification of the or in 1.3. Is the entity identifying low impact BCS or supporting SCI or both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?

We don’t understand how to categorize a Shared Cyber Infrastructure. The SDT seems to make a distinction between two types of SCI, one type is supporting, and the other type is independent supporting. Our hypothesis is that a “supporting SCI” is for BCS (BCA/PCA) and that an “independent supporting SCI” is for associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS)).

In both cases, the SCI is the categorization labels, like BCA, PCA, EACMS, PACS, TCA.

Yet in the Applicable Systems column in the other CIPs, the SDT seem to make a distinction between the SCI, for example

CIP-005 R1.5 1.5 … PACS hosted on SCI … SCI identified independently…

CIP-007 R1.1 SCI identified independently supporting.

Clarification is needed.

Are the two options for identification SCI required? Is there a difference in the controls that we want to apply?

We suggest simplifying the language or add more precision. Example:

Per Attachment 1, Section 1, identify each high impact BES Cyber System as either of the following, if any, at each asset; High Impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs) or SCI.

Furthermore, in the definition of SCI the PCA is not listed. Is this intentional? Wouldn't be possible to have a PCA supported by an SCI? We suggest that the SDT review the SCI / VCA/ PCA definitions, adjust the applicability and the requirements.

Reference SCI: One or more programmable electronic devices, including the software and Management Interfaces, that share: • CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The ISO/RTO Council (IRC) Standards Review Committee (SRC) requests clarification of how SCI is to be treated when it supports both high impact BES and medium impact BES; i.e. is the SCI to be watermarked to the highest impact?

Request clarification of "it is a part of for CIP Requirement Applicability?" Is there a missing word? Should the language be "it is a part of it for CIP Requirement Applicability?"

Request clarification of the OR in 1.3. Is the entity identifying low impact BCS OR supporting SCI OR both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	Yes
Document Name	

Comment

Chelan approves of this language.

Likes 0	

Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
The shared SCI and TCA definitions are clear and are understood by technical staff; however, the scope included in these definitions may be dfficult to communicate to management staff as written.	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the two options for identification of SCI within CIP-002 are clear.	
Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
ACES agrees when SCI is included in the CIP Systems it falls into scope of CIP requirements where SCI is an Applicable System. The issue is not with CIP-002's usage of SCI or its definition, but the definition of CIP System as it lacks the inclusion of VCAs which could lead to confusion. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) agrees that the two options in CIP-002 R1 are clear, due to the explanation in the Technical Rationale, and understands that SCI is an applicable system when it supports an applicable system either as part of the system or as independent SCI.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Southern Indiana Gas and Electric Company (SIGE) agrees that the two options in CIP-002 R1 are clear, due to the explanation in the Technical Rationale, and understands that SCI is an applicable system when it supports an applicable system either as part of the system or as independent SCI.	

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	

Response
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment
Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response
Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	Yes
Document Name	

Comment
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	

Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Yes. The two options for SCI identification are clear within the CIP-002 standard revisions. However, the SDT should provide implementation guidance including examples of how to document the SCI, whether included within the CIP System or independently. Additionally, it would be helpful if the SDT was able to provide Implementation Guidance that included a logic diagram depicting how the device classifications and embedded definitions like Management Interface and CIP System can be applied. In addition, the SDT has been clear that this project focuses on on-premise virtualization, however, many virtualization concepts, like SCI, could be interpreted as being related to use of cloud computing technologies. AWS suggests explicitly stating that the Standards do not apply to cloud within the Applicability section of CIP-002. If these updated Standards do not apply to cloud, it should be obvious to the reader.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees that the two options are clear and it is understood that when a high/medium impact BCS that includes any supporting SCI is identified as a complete BCS (‘all-in’), the SCI is included in CIP requirement applicability wherever a BCS is identified in applicability.	
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 two options in CIP-002 R1 are clear based on the explanation contained in the technical rationale, and supports the changes made regarding the identification of SCI within CIP-002.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
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	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	

Answer	Yes
Document Name	2016-02_Virtualization_Unofficial_Comment_Form_(FINAL).docx
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. The Applicable Systems column may include "SCI identified independently…" Is this clear or is additional clarification (such as "SCI identified as supporting, but not part of…") needed?

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The existing language, "SCI identified independently supporting an Applicable System" is open to misinterpretation. The IRC SRC recommends the language be clarified by adding a comma to distinguish between "identified independently" and "supporting" as follows: "SCI identified independently, supporting an Applicable System"

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

This language can be misinterpreted. Recommend clarification. Current language is "SCI identified independently supporting an Applicable System." Suggest adding a comma to distinguish between "identified independently" and "supporting." Resulting in "SCI identified independently, supporting an Applicable System"

The context of the question isn't clear is this question a general question or it's pertaining to CIP-002.

Also, the question offers two choices; "Is this clear" or "is additional clarification needed" yet the choices are Yes/No.

So, our answer; is No, it's not clear and yes additional clarification is needed.

Our hypothesis is that it must be a general question. We are not sure of the value of identifying the SCI ("supporting SCI" vs an "independent supporting SCI"), the SCI should be controlled and own requirements.

If the SDT maintains its distinction, they should enforce two types of categorizations and the requirements should be defined with those two types of categorizations in mind.

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Additional guidance is needed for “SCI identified independently.” Also, the phrase “independent SCI supporting…” is not clear. Is this specifically to the VM environment used to create the virtual BCS?	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	

Comment
PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	

Comment
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	

Comment
Additional clarification such as mentioned in Question 1 comment would be a benefit. Also, additional clarity regarding how to group or identify the SCI objects would be beneficial. By chassis, by blade, by host, by logical grouping of functions, etc.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	

Comment
The process for the independent identification of SCI is not clear and needs additional clarification. EEI notes that within the VSLs for CIP-002, “independently identified SCI” is mentioned 27 times, yet no explanation is provided as to what it means or how this is to be accomplished. It is also not clear what is meant by the term “independent SCI”. This term is prominently used in Requirement R1, subpart 1.1 and 1.2 (bullet 2) but not explained. EEI asks that the SDT either define the term or use another term that is more widely understood. **Note:** While EEI has identified our concern related to the use of SCI identified independently in CIP-002, this phrase is used throughout the CIP standards. For this reason, the SDT should provide more clarity to this term.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	

Comment
ERCOT supports the IRC SRC comments and offers these additional comments: • Clarify “identified independently supporting”. It is unclear what this means. Independent of what? • Listing the SCI in the applicable systems columns contradicts what was done in the definition of BES Cyber System. The proposed definition of BES Cyber System already includes SCI but does not have the same qualifiers as in the applicable systems column.

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 agrees that “SCI identified independently” is clear and no additional clarification of that particular phrase is needed. However, Southern is concerned with the lack of clarity around SCI that does not host a BES Cyber System and is not within an ESP. Specifically, the inclusion of EACMS and PACS within the definition of SCI (and SCI within the EACMS and PACS definitions). As an example, an entity may have a VCA that is involved in processing access control logs. If this is an example of the “M” in EACMS (see discussion of this on Q14), and any part of the process executes as a VCA, then is the entire SCI now in scope? If so, what about backup systems that copy off snapshots of VCA for backup and thus may “share storage resources” with an EACMS? It is not clear where the scope of this “EACMS” ends. Southern believes there is clarity and simplicity for SCI that hosts a BCS and is in an ESP, but suggests scoping SCI to that which hosts a BCS and creating separate requirements to specifically address access to the

mgt plane of an EACMS or PACS, for example (however, see Q14 as even that is problematic with the broadness of EACMS). This would be much more straightforward than treating SCI outside the ESP the same as SCI hosting a BCS.

Southern proposes the following alternative language for defining SCI, EACMS and PACS:

SCI: One or more programmable electronic devices, including the software and Management Interfaces, that share:

- CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA; or
- storage resources with any part of a BES Cyber System.

Each SCI is either:

- included in one or more BES Cyber Systems; or
- identified independently.

SCI does not include the supported VCA or CA with which it shares its resources.

EACMS: Cyber Assets or Virtual Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems.

PACS: Cyber Assets or Virtual 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.

Likes 0	
Dislikes 0	

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer	No
Document Name	

Comment

<duplicate>

Likes 0	
Dislikes 0	

Response

Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	
Eversource recommends using "Independently identified". The term seems inconsistent in regards to how its used in all the CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
While it is clear to those that have been following this project and or understand virtualization technologies and how it is used, a non-technical person may need more clarification. Further, “SCI identified independently…” the information provided in the most recent webinar was much clearer than what reads in the standards and Technical Rationale, but that is not binding. While both try to explain it, we don’t feel the Technical Rationale and glossary term does enough to distinguish exactly what is intended by the SDT. Secondly, CIP-002 R1.x doesn’t use the same verbiage. For example, “A XXXX impact BCS and independent SCI supporting any part of the XXXX impact BCS...” This should read: “A XXXX impact BCS and any SCI identified independently… supporting any part of the XXXX impact BCS...” We do feel these two classifications could work for industry, but need significant and binding definitions and distinctions with technical basis so entities can avoid misclassification of SCI.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	

Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
Requesting better clarification as industry may misinterpret especially the SCI “form” relationship to a function.	
Likes 0	
Dislikes 0	
Response	

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
The draft language is not clear. We assume that the phrase means SCI not declared as part of a BCA, PCA, EACMS, or PACS but it supports the BCA, PCA, EACMS, or PACS function (for example, a BCA can be run on VM system and the VM system will be defined as SCI, and the SCI can be declared as only SCI and not a dual declaration as a BCA and a SCI). However, this is only an assumption. How can SCI can both be independent and supporting any part of a BES Cyber System? If SCI supports any part of a BES Cyber System then it is not independent and is supporting.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Not clear on how the SCI is defined in this scenario. For the definition of "SCI identified indepently" is unclear what is meant by this definition, and is not clearly spelled out but an assumption is made. It appears to be assumed that the phrase means SCI not declared as part of a BCA, PCA, EACMS or PACS but it supports the BCA, PCA, EACMS, or PACS function. Would like this clearly spelled out by defintion and by each of the Applicable Systems column.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	No
Document Name	
Comment	
Additional guidance is needed for “SCI identified independently.” Also, the phrase “independent SCI supporting…” is not clear. Is this specifically to the VM environment used to create the virtual BCS?	

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

"SCI identified independently" is not clear and needs additional clarification.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

This language can be misinterpreted. Recommend clarification. Current language is "SCI identified independently supporting an Applicable System." Suggest adding a comma to distinguish between "identified independently" and "supporting." Resulting in "SCI identified independently, supporting an Applicable System"

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Please provide additional clarification with respect to Applicable Systems callout for SCI beyond the phrase "SCI identified independently...".

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

Additional guidance is needed for “SCI identified independently.” Also, the phrase “independent SCI supporting…” is not clear. Is this specifically to the VM environment used to create the virtual BCS?

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5

Answer	No
Document Name	

Comment

Additional clarification is needed.

Recommend spelling out "Shared Cyber Infrastructure" and its acronym within the standard text.

Recommend including the definition within the text, or make a statement in the text directing to the definition in the definition list.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The language “SCI identified independently” is not clear and should be removed from CIP-002 to CIP-013 (see our comments 1 in Q1). Resulting from our proposed changes to the definitions in Q1, the language “SCI identified independently” is no longer needed. A SCI should be identified either as one of the existing CIP cyber assets or out of CIP cyber asset scope.

This is not clear. We assume that the phrase means SCI not declared as part of a BCA, PCA, EACMS, or PACS but it supports the BCA, PCA, EACMS, or PACS function (for example, a BCA can be run on VM system and the VM system will be defined as SCI, and the SCI can be declared as only SCI and not a dual declaration as a BCA and a SCI). However, this is only an assumption.

Further, the phrase “independent SCI supporting any part of the … BCS” is confusing. It is not clear how an SCI can both be independent and supporting any part of a BES Cyber System. On its face it would seem that if an SCI supports any part of a BES Cyber System then it is not independent and is supporting.

We acknowledge the SDT’s attempt to avoid a “hall of mirrors” scenario where it could be interpreted that a device serving as an EACMS is required to have its own EACMS. However we also feel this situation may already occur today in some audits and not just a possibility going forward in the future. We recommend modifying existing definitions of BES Cyber System, BES Cyber Asset, and/or EACMS (ex. including an exclusionary phrase that an EACMS does not require its own EACMS).

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

This language can be misinterpreted. Recommend clarification. Current language is “SCI identified independently supporting an Applicable System.” Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

The context of the question isn’t clear is this question a general question or it’s pertaining to CIP-002.

Also, the question offers two choices; “Is this clear” or “is additional clarification needed” yet the choices are Yes/No.

So, our answer; is No, it’s not clear and yes additional clarification is needed.

Our hypothesis is that it must be a general question. We are not sure of the value of identifying the SCI (“supporting SCI” vs an “independent supporting SCI”), the SCI should be controlled and own requirements.

If the SDT maintains its distinction, they should enforce two types of categorizations and the requirements should be defined with those two types of categorizations in mind.

Likes 0	
Dislikes 0	

Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP fully supports EEI's comments that the process for the independent identification of Shared Cyber Infrastructure (SCI) is not clear and needs additional clarification.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
In support of NPCC RSC comments This language can be misinterpreted. Recommend clarification. Current language is "SCI identified independently supporting an Applicable System." Suggest adding a comma to distinguish between "identified independently" and "supporting." Resulting in "SCI identified independently, supporting an Applicable System"	

The context of the question isn't clear is this question a general question or it's pertaining to CIP-002.

Also, the question offers two choices; "Is this clear" or "is additional clarification needed" yet the choices are Yes/No.

So, our answer; is No, it's not clear and yes additional clarification is needed.

Our hypothesis is that it must be a general question. We are not sure of the value of identifying the SCI ("supporting SCI" vs an "independent supporting SCI"), the SCI should be controlled and own requirements.

If the SDT maintains its distinction, they should enforce two types of categorizations and the requirements should be defined with those two types of categorizations in mind.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Additional guidance is needed for “SCI identified independently.” Also, the phrase “independent SCI supporting…” is not clear. Is this specifically to the VM environment used to create the virtual BCS?	
Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
If the language “SCI identifieid independently” is used then it would be beneficial for “identified independently” to be explicitly defined.	
Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	

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

Document Name	
Comment	
We support NPCC TFIST's comments as found below: This language can be misinterpreted. Recommend clarification. Current language is “SCI identified independently supporting an Applicable System.” Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	

Answer	No
Document Name	
Comment	

The definition of Shared Cyber Infrastructure (SCI) will be better explained with the term “SCI identified as supporting, but not part of…”.

BC Hydro requests that SDT provide more clarity around the concept of "not part of.." to better understand the separation point between whether an SCI is considered supporting but not actually part of BCAs, PCAs, EACMS or PACS.

BC Hydro also requests that SDT include a couple of practical examples to explain this concept within the Technical Rationale and proposed definition of SCI.

Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	
Comment	

It is not clear what is meant by “SCI identified independently…”

Likes 0	
Dislikes 0	
Response	

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	
Comment	

SIGE finds the language “SCI identified independently supporting an Applicable System above” confusing. It is confusing because “SCI identified independently” is a process, and CIP-002-7 R1.1 uses the term “independent SCI” when it asks to identify, “A high impact BCS and independent SCI supporting …” When stated in this context, the phrase “independent SCI” is a thing that can be defined. SIGE proposes that the Applicable Systems column should state “Independent SCI that supports an Applicable System above” and that “independent SCI” can be defined or explained as “a Cyber System identified separately from the BCS, EACMS, PACS, and/or PCA it supports.”

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA does not support the definition and raises the question how SCI is to be identified independently. At there very least there would need to be guidance on what should be considered in the identification process.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE finds the language “SCI identified independently supporting an Applicable System above” confusing. It is confusing because “SCI identified independently” is a process, and CIP-002-7 R1.1 uses the term “independent SCI” when it asks to identify, “A high impact BCS and independent SCI supporting …” When stated in this context, the phrase “independent SCI” is a thing that can be defined. CEHE proposes that the Applicable Systems column should state “Independent SCI that supports an Applicable System above” and that “independent SCI” can be defined or explained as “a Cyber System identified separately from the BCS, EACMS, PACS, and/or PCA it supports.”

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Additional clarification is needed as “SCI identified independently…” remains ambiguous.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	

Comment

The phrase “independent SCI supporting any part of the … BCS” is confusing. It is not clear how an SCI can both be independent and supporting any part of a BES Cyber System. On its face it would seem that if an SCI supports any part of a BES Cyber System then it is not independent and is supporting.

We acknowledge the SDT’s attempt to avoid a “hall of mirrors” scenario where it could be interpreted that a device serving as an EACMS is required to have its own EACMS. However we also feel this situation may already occur today in some audits and not just a possibility going forward in the future. We recommend modifying existing definitions of BES Cyber System, BES Cyber Asset, and/or EACMS (ex. including an exclusionary phrase that an EACMS does not require its own EACMS).

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

While it is clear to those that have been following this project and or understand virtualization technologies and how it is used, a non-technical person may need more clarification. Further, “SCI identified independently…” the information provided in the most recent webinar was much clearer than what reads in the standards and Technical Rationale, but that is not binding. While both try to explain it, we don’t feel the Technical Rationale and glossary term does enough to distinguish exactly what is intended by the SDT.

Secondly, CIP-002 R1.x doesn’t use the same verbiage. For example, “A XXXX impact BCS and independent SCI supporting any part of the XXXX impact BCS...” This should read: “A XXXX impact BCS and any SCI identified independently… supporting any part of the XXXX impact BCS...”

We do feel these two classifications could work for industry, but need significant and binding definitions and distinctions with technical basis so entities can avoid misclassification of SCI.

AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Additional clarification is needed	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
The phrase “SCI Identified Indepedently, and more generally the desfinition of SCI is ambiguous and It is confusing to understand the definition of Shared Cyber Infrastrure (SCI) and therefore the overall requirement is unclear. Is SCI watermarked at the highest level? Strongly encourage better definition within the language of the standard and definitions to ensure that implementation is not dependent on independent on non-enforcable technical rationale and implementation guidelines.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	

AZPS feels that “SCI identified as supporting, but not part of” provides more clarity than “SCI identified independently…”, as it could be interpreted as applied to an SCI that is only supporting an applicable system.

We feel the statement “SCI that supports an applicable system that is independently categorized as an SCI and as not part of the applicable BES Cyber System” provides more clarity.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	No
Document Name	

Comment

This is already clarified in the third and fourth bullet of the SCI definition. Suggest using ‘SCI supporting an Applicable System above.’ See (CIP-005-8 Part 1.5)

Likes 0	
Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5

Answer	No
Document Name	

Comment

This is not clear. We assume that the phrase means SCI not declared as part of a BCA, PCA, EACMS, or PACS but it supports the BCA, PCA, EACMS, or PACS function (for example, a BCA can be run on VM system and the VM system will be defined as SCI, and the SCI can be declared as only SCI and not a dual declaration as a BCA and a SCI). However, this is only an assumption.

Further, the phrase “independent SCI supporting any part of the … BCS” is confusing. It is not clear how an SCI can both be independent and supporting any part of a BES Cyber System. On its face it would seem that if an SCI supports any part of a BES Cyber System then it is not independent and is supporting.

We acknowledge the SDT’s attempt to avoid a “hall of mirrors” scenario where it could be interpreted that a device serving as an EACMS is required to have its own EACMS. However we also feel this situation may already occur today in some audits and not just a possibility going forward in the future. We recommend modifying existing definitions of BES Cyber System, BES Cyber Asset, and/or EACMS (ex. including an exclusionary phrase that an EACMS does not require its own EACMS).

Likes 0	

Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	

Comment
See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	

Comment
Introduction of the SCI Group concept as enumerated in response to Question 1 would provide the further clarity needed to address the relationship of devices identified as SCI to the BCS or SCIG of which they are a member. This additional clarity should be reinforced in the definitions, proposed as follows: **DUKE ENERGY PROPOSED DEFINITIONS FOR BCS, SCI, and SCIG:** **BES Cyber System (BCS) -** One or more BES Cyber Assets logically grouped by a Responsible Entity to perform one or more reliability tasks for a functional entity, including Shared Cyber Infrastructure that the Responsible Entity chooses to group into the BES Cyber System it supports. **Shared Cyber Infrastructure (SCI) -** Programmable electronic devices, including the software and Management Interfaces, that share…(proposed bullets remain)… Each SCI is grouped by the Responsible Entity into one or more BCS or SCIG. SCI does not include the supported VCA or CA with which it shares its resources. **Shared Cyber Infrastructure Group (SCIG) -** One or more Shared Cyber Infrastructure devices logically grouped by a Responsible Entity.

Likes 0	
Dislikes 0	

Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Additional clarification is required. Some SCI may provide underlying compute, storage, or network virtualization services, which is essential for the proper function of a BCS. Other SCI systems such as those providing overlays for management functions or monitoring, may not be required for real-time BCS functionality. Accordingly, that distinction, and provision of controls accordingly, would be beneficial in the associated glossary terms.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
The Applicable System, “SCI identified independently” is ambiguous and unclear at best. Specifically, if SCI is hosting multiple Applicable Systems of different ratings, how is the SCI to be classified? Should it be high watermarked and protected to the highest rating of those Applicable Systems? If so, the SCI should be classified at the high watermark and be afforded the same protections as the Applicable System it supports - BCS, EACMS, PACS. The current definition and requirement is ambiguous which could result in an interpretation that applies BCS controls to an SCI that only supports EACMS or PACS. NRG requests the Standards Drafting Team provide more clarity between the two options: “All in” and “Identified SCI Option” as they seem to apply only when supporting a BCS and not in instances where SCI is hosting EACMS and/or PACS only. NRG disagrees with	

the Technical Rationale that requires logical isolation of SCI that hosts EACMS/PACS and no impact cyber systems. Within the context of the current CIP standards, there is no requirement for logical isolation between physical servers in this scenario.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
The Applicable System, “SCI identified independently” is ambiguous and unclear at best. Specifically, if SCI is hosting multiple Applicable Systems of different ratings, how is the SCI to be classified? Should it be high watermarked and protected to the highest rating of those Applicable Systems? If so, the SCI should be classified at the high watermark and be afforded the same protections as the Applicable System it supports - BCS, EACMS, PACS. The current definition and requirement is ambiguous which could result in an interpretation that applies BCS controls to an SCI that only supports EACMS or PACS. NRG requests the Standards Drafting Team provide more clarity between the two options: “All in” and “Identified SCI Option” as they seem to apply only when supporting a BCS and not in instances where SCI is hosting EACMS and/or PACS only. NRG disagrees with the Technical Rationale that requires logical isolation of SCI that hosts EACMS/PACS and no impact cyber systems. Within the context of the current CIP standards, there is no requirement for logical isolation between physical servers in this scenario.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	No
Document Name	
Comment	
The term "SCI identified independently" does not read intuitively without reading the guidance and technical rationale. Since those documents are not auditable, it must stand on its own and needs more revision to be more clear. Consider developing an additional defined term and classification: "Independent SCI" - "An SCI that is not identified as part of a BCS or its associated EACMS, PACS, or PCAs." This approach would keep the requirement language clean and include the needed guidance in the auditable parts of the standards and definitions.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy recommends modifying the definition as folows: “SCI identified as supporting **the functionality,** but not part of…”.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends adding the additional clarification (such as “SCI identified as supporting, but not part of…”).	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes

Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Yes, it is clear that the “SCI identified independently” means that it is supporting any part of a high or medium impact BCS or associated EACMS, PACS or PCAs and is not included in the BCS. However, since “SCI identified independently…” is explicitly listed in the applicability columns, the other option for SCI to be included within the CIP System should also be explicitly stated. For example, “High Impact BCS, including supporting SCI, and their associated…”.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
: **GSOC recommends revising the language in the definition of SCI such that it is clear to registered entities that “Each SCI must be identified as either…” As well, when SCI is addressed within other definitions, requirements, or applicable systems columns, consistent language should be used throughout, i.e., within the body of the standards, within the definitions, and between the definitions and the standards. As an example of inconsistencies identified in the new definitions, SCI is characterized as “supporting,” “included in,” or “grouped in/with” in various definitions, which usage may not comport with the terms used in the definition of SCI. Additionally, in CIP-002, SCI is referenced as “supporting” or “independent supporting,” but the term “supporting” is not utilized in the definition of SCI nor in its potential charcterizations as set forth in the definition. Finally, SCI reference language included in CIP-006 and other standards, at times, includes a clarifications to ensure exclusion of those SCI grouped into a BCS, but that language is also not consistently applied throughout the standards. To ensure clarity, it is recommended that the language utilized to reference SCIs is consistent throughout the definitions, throughout the standards, and between the definitions and standards.**	
Likes 0	

Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Yes, although PNMR agrees with EEI that the term "independent SCI" should be clearly explained.	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Yes, this is clear.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. The SDT modified the ERC definition to reference "outside the asset containing". This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

There is insufficient clarity provided within the proposed terms to ensure consistent understanding and identification of applicable traffic.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Duke has identified three concerns with the proposed ERC definition and underlying strategy:

First, the "outside the asset containing" language expands the current ambiguity in CIP-003 to High and Medium sites, allowing for auditor interpretation with respect to how communication that is translated or terminated through a bastion host locally at the asset should be assessed. It is not clear from the definitions whether the SDT intends that communication from an outside location that first terminates on a non-CIP System at the asset and then

pivots to a CIP System at the asset is included in this ERC definition, or if that break in communication is basis to exclude the CIP System from the ERC applicability.

Second, use of the ERC definition to attempt to address security concerns associated with remote access to devices that are accessible based on Serial to IP conversion alone exacerbates the CIP-004, 006, and 007 scoping challenges noted by the SDT.

The ERO has socialized a better path forward using the IRA definition to ensure that devices accessible in this manner are correctly secured. This would be a better strategy for securing these assets while minimizing low-value compliance paperwork (e.g. documenting lack of syslog capability on a serial-only relay). This change would take the SDT's removal of ERC from the CIP-005 requirement language to its logical conclusion, removing the dependence on the ERC definition to define security posture and instead using it as a scoping tool. Refer to slides 9-11 in following presentation: https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20RF/2016-02_ERC_and_IRA_Webinar_Slides_05072020.pdf

Third, the use of CIP Systems creates confusion as there are no ERC requirements applied to other classifications of devices that are included in the CIP Systems definition (e.g. EACMS, PACS, and TCA devices). Although simplicity in definitions is desirable, it would be clearer to spell out the system types that are relevant to the defined term (e.g. BCS, PCA, SCI).

Therefore, Duke proposes the following definition of ERC, which incorporates the SDT's improved "communicate" terminology while remaining focused on the ESP boundary as the point where the determination is made.

External Routable Connectivity (ERC) - The ability to communicate across a defined ESP via a bi-directional routable protocol connection.

It does not appear that the SDT's rationale regarding the shrinkage of the ESP in Zero Trust environments is likely to reach the intra-device level given that the CA, VCA, and SCI definitions remain device-centric. Therefore, Duke strongly feels that the fundamental change proposed by the SDT is not justified by the potential downside the SDT has identified.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	No
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	

Just as it has been problematic for entities with assets containing low impact BES Cyber Systems to identify where electronic access controls must be afforded for routable protocol, the use of a physical construct for where logical controls are implemented for CIP-004 and CIP-006 appears to further the problem.

Consider the following two edit to the proposed ERC definition:

The ability to communicate to a CIP System using a bi-directional routable protocol from a nonCIP System.

Likes 0	
Dislikes 0	
Response	

William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	

The lower-case ‘asset’ used in the definition really erodes the intent of ERC. This could allow an entity to not consider communication between corporate networks and BCS to be ERC if they are in the same building (‘asset’), for example at a Control Center. Alternative proposal: *The ability to communicate to a CIP System using a bi-directional routable protocol from a Cyber System that is not protected by an Electronic Security Perimeter located at the same asset. However, the alternate proposal still has a limitation on ‘asset’, which is an undefined term.*

Likes 0	
Dislikes 0	
Response	

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	

AZPS feels that changing the language to “communicate to” instead of “accessing” has the potential to expand the scope of ERC unintentionally. Including “outside the asset containing the CIP system” leads to ambiguity while use of ESP helps clarify intent. The new definition suits virtual fully, but leaves vagueness and abiguity to physical aspects. AZPS respectfully recommends creating two separate definitions for physical and virtual.

Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
The new language does not clarify where the border where bi-directional communication is considered. The current definition, which specifies the border to be at that EACMS (local firewall) is adequate for most cases. We understand that the definition needs to be adjusted to recognize implementation of zero trust models. However, clarifying that external routable connectivity is determined at the physical border of the asset would clearly identify where external routable connectivity is to be considered.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Additional clarification is needed	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
ACES does not agree with the reference “outside the asset containing” as a scoping mechanism for CIP-007 R4. We do not understand the correlation of ERC to CIP-007 logging or CIP-004 and CIP-006 risks. Using the “asset” as a scoping mechanism could lead to various interpretations and allow for	

loop holes for access. In our opinion, “outside the asset containing” is not necessary to define ERC. We feel ESP is still the proper scoping mechanism.

AEPC has signed on to ACES comments.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE does not agree with the proposed change to the ERC definition because the phrase “from outside the asset containing the CIP System” is not clear. “Asset” is not a term in the NERC Glossary of Terms; therefore the definition cannot clarify precisely what “outside the asset” means. Is it a room, building, geographical location, or something else?

In addition, the proposed definition greatly expands the existing definition by changing from “BES Cyber System” to “CIP System” and by changing from “... to access …” to “… to communicate …”. However, this expansion can be controlled by specifying specific Cyber Systems in the requirements.

CEHE suggests maintaining the currently approved definition until a more clearly defined proposal is offered or “Asset” is added as a defined term in the NERC Glossary.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA does not support the phrase “outside the asset” is vague and confusing. NCPA suggests the change “…ability to communicate to a CIP System using bi-directional routable protocol from a separate asset containing the CIP system.”

Likes 0	
Dislikes 0	

Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree with the proposed change to the ERC definition because the phrase “from outside the asset containing the CIP System” is not clear. “Asset” is not a term in the NERC Glossary of Terms; therefore the definition cannot clarify precisely what “outside the asset” means. Is it a room, building, geographical location, or something else? In addition, the proposed definition greatly expands the existing definition by changing from “BES Cyber System” to “CIP System” and by changing from “... to access …” to “… to communicate …”. However, this expansion can be controlled by specifying specific Cyber Systems in the requirements. SIGE suggests maintaining the currently approved definition until a more clearly defined proposal is offered or “Asset” is added as a defined term in the NERC Glossary.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	
It’s not clear what is meant by the phrase “from outside the asset containing the CIP System.” This makes it sound like all CIP Systems must reside within a electronic security perimeter. It is unclear what it is that the SDT is attempting to accomplish with this wording or how it is allowing scoping based on connectivity of the logging systems as required by CIP-007. Further, the use of the term “asset,” with a lower case A, often causes confusion with “Cyber Asset” when discussing requirements with SMEs.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No

Document Name	

Comment

Texas RE is concerned the new proposed changes to the ERC definition only focus on WAN and excludes LAN network communications. LAN and WAN network communications are both captured under the current definition. If the proposed changes are approved, registered entities could potentially argue that they have no ERC even though a bi-directional routable protocol connection is being utilized from LAN to LAN.

As such, this change could reduce the entities' overall security posture by placing such communications potentially outside the scope of the entities' CIP-program. For example, the proposed language for CIP-005 R2.1 includes in scope "medium impact BCS with ERC". Since the proposed ERC definition focuses on the term "asset", Texas RE is concerned that entities could potentially read the "asset" language to remove from scope BCAs such as operator consoles that are not accessible from outside the Control Center (that is, from outside the "asset"). Specifically, because there is no ERC from outside of the Control Center, it could be argued that the operator consoles no longer fall within the proposed ERC definition. As a result, important CIP protections such as the use of an Intermediate System to access those assets, physical protections, and personnel training requirements would be limited.

Given these concerns, Texas RE recommends retaining the current definition of ERC.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

BC Hydro seeks more clarity on the term "asset" in relation to the reference "outside the asset containing." Specifically, it is not clear whether the term "asset" is meant to talk to individual BES Elements (i.e. a specific transformer, circuit breaker, etc.) or whether entities are given the latitude to define the boundaries of assets (i.e. could be based on defined physical boundaries of a broader transmission or generation station or a Control Centre). Recommend providing specific drawing examples similar to the models provided under the CIP-003-8 standard to help visualize through practical network architecture to characterize what would constitute ERC under this new proposed definition.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No

Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: We understand that “outside the asset containing” is a scoping mechanism. Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement? We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary? Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?	
Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
The modification to the definition to ERC brings serially connected OT Devices using a protocol-converter into scope for multiple CIP-007 requirements. In some instances, compliance with all CIP-007 requirements would be impossible. The use of a protocol converter does not facilitate centralized logging, review, and alarming (based on events). It simply facilitates data acquisition and IRA to these devices. We suggest not revising the definition of ERC, leaving the concept of a protocol break in place and require the protocol converter to either be categorized as a BCA, PCA or EACMS (depending on the circumstance). The serial OT device could still utilize the proposed definition for IRA to be in scope for CIP-005.	
Likes 0	
Dislikes 0	

Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	

Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
The proposed change to the ERC definition expands scope by making the boundary physical “asset” from the original electronic concept. ERC could happen within a room where two systems have discrete ESPs that communicate between each other. Change the ability to “access” to “communicate to” to bring the connectivity rationale into the term.	

Suggested definition - *The ability to communicate to a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.*	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
In support of NPCC RSC comments.	

We understand that “outside the asset containing” is a scoping mechanism.

Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement?

We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary?

Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?

The overall definition of ERC is

The ability to communicate to a CIP System using a bi-directional routable protocol from outside the asset containing the CIP System.

(The definition of CIP System is included for precision)

The ability to communicate to a CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.) using a bi-directional routable protocol from outside the asset containing the CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.).

We don’t see the added value of this “scoping” for CIP-007 R4, CIP-004, CIP-006. This definition includes additional asset types (EACMS, PACS, SCI, PCA, TCA) to the concept of ERC. One could think that future requirements could come forward, like for EACMS with ERC or even TCA with ERC, but it’s not the case.

In reference to CIP-007 R4, the text used is the following

Medium Impact BCS with External Routable Connectivity and their associated:

1. EACMS;

2. PACS; and

3. PCA

SCI identified independently supporting an Applicable System above

The ERC trigger is still based on the BCS.

If the understanding of asset (“the asset containing “) is equivalent to the following … i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. RAS that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above… the suggested definition is interesting.

Our comprehension is that if we have two HIGH/Medium-Impact BCS in the same Control Center (asset) using a bi-directional routable protocol to establish their communication and that any of those BCS doesn’t use a bi-directional routable protocol outside of the Control Center, the ERC definition wouldn’t be applied. Furthermore, if any of those two BCS would be using a bi-directional routable protocol outside of the asset of both BCS would be tagged as being ERC.

We suggest the removal of CIP System in the definition.

Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP does not support the proposed changes to the External Routable Connectivity (ERC) definition and is in support of EEI's comments. The new definition for ERC expands the scope by (1) replacing the defined term "BES Cyber System (BCS)" with a proposed new term "CIP System", and (2) changing "the ability to access …" to "the ability to communicate to …". In addition, AEP seeks additional clarification on "asset containing the CIP System". The term "asset" could be interpreted in many ways and could be a point of contention if an entity identified an "asset" at a fence line where an auditor may have a different opinion on where that line of demarcation for an "asset" might be drawn.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
We understand that "outside the asset containing" is a scoping mechanism.	

Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement?

We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary?

Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?

The overall definition of ERC is

The ability to communicate to a CIP System using a bi-directional routable protocol from outside the asset containing the CIP System.

(The definition of CIP System is included for precision)

The ability to communicate to a CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.) using a bi-directional routable protocol from outside the asset containing the CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.).

We don't see the added value of this "scoping" for CIP-007 R4, CIP-004, CIP-006. This definition includes additional asset types (EACMS, PACS, SCI, PCA, TCA) to the concept of ERC. One could think that future requirements could come forward, like for EACMS with ERC or even TCA with ERC, but it's not the case.

In reference to CIP-007 R4, the text used is the following

Medium Impact BCS with External Routable Connectivity and their associated:

1. EACMS;

2. PACS; and

3. PCA

SCI identified independently supporting an Applicable System above

The ERC trigger is still based on the BCS.

If the understanding of asset ("the asset containing ") is equivalent to the following … i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. RAS that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above… the suggested definition is interesting.

Our comprehension is that if we have two HIGH/Medium-Impact BCS in the same Control Center (asset) using a bi-directional routable protocol to establish their communication and that any of those BCS doesn't use a bi-directional routable protocol outside of the Control Center, the ERC definition wouldn't be applied. Furthermore, if any of those two BCS would be using a bi-directional routable protocol outside of the asset of both BCS would be tagged as being ERC.

We suggest the removal of CIP System in the definition.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
We disagree to modifying ERC definition. Given that the ESP is still effective and the language BCS with ERC and IRA are still used by STD in the revised requirements, ERC should be still ESP and BCS based rather than asset based. If using the physical boundary to identify ERC, it is hard to decide which BCS with ERC and which BCS without ERC, which would cause ERC identification issues and various interpretations. Also the asset boundary will cause the security risk since the highwater marking wouldn't apply within a physical boundary. Furthermore, physical boundary would cause audit issue since it is not a defined term. For instance, whether a generating station power house and its switchyard are treated as the same asset or separate asset will get the different results. In addition, the proposed ERC definition overreaches the goal of SAR since the revised ERC refers to CIP System which includes all types of CIP cyber assets. The SRA doesn't require entities to identify ERC for EACMS, PACS, and TCA that are outside ESP. **Recommendation:** Restore the current ERC definition since it still fits the revised requirements.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	

Comment
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

The proposed change to the ERC definition expands scope by making the boundary physical “asset” from the original electronic concept. ERC could happen within a room where two systems have discrete ESPs that communicate between each other.

Change the ability to “access” to “communicate to” to bring the connectivity rationale into the term.

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

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment
In support of IRC SRC/SWG. We understand that “outside the asset containing” is a scoping mechanism. Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement? We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary? Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	No
Document Name	

Comment
The proposed change to the ERC definition expands scope by making the boundary physical “asset” from the original electronic concept. ERC could happen within a room where two systems have discrete ESPs that communicate with each other. Change the ability to “access” to “communicate to” to bring the connectivity rationale into the term. Suggested definition - *The ability to communicate to a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.*

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	

Comment
We support EEI's comments on this question.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Because the term and concept of ESP remains effective and the BCS language of ERC and IRA are used by STD in the revised requirements, ERC should remain ESP and BCS based rather than asset based. It is difficult to determine which BCS with ERC and which BCS without ERC would apply with the proposed language.

The asset boundary will cause a security risk since the highwater marking wouldn't apply within a physical boundary. Furthermore, physical boundary would cause audit issue since it is not a defined term. For instance, whether a generating station power house and its switchyard are treated as the same asset or separate asset will get the different results. In addition, the proposed ERC definition overreaches the goal of SAR since the revised ERC refers to CIP System which includes all types of CIP cyber assets. The SRA doesn't require entities to identify ERC for EACMS, PACS, and TCA that are outside ESP.

Recommendation: Restore the current ERC definition since it still fits the revised requirements.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- The proposed change for ERC is confusing, including March and August discussions with the SDT during outreach, for when a CIP System that serial converts RS-232 or RS-485 may extend ERC beyond the ESP to medium impact BCAs, PCAs and Non-CIP Cyber Asset. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation.
    - Where is the electronic boundary and how does it apply when not routable?
    - Where is the physical boundary when serial extends out of the substation to field devices?
    - When does ERC apply to a CIP System that is connected serially that was previously consider non-routable before the new proposed updates from Project 2016-02 SDT?
        - Please clarify the language that extends applicability to a CIP System using serial communication within the asset/site?

- If the serial link can change the configuration of a BCA is the SDT intending Entities now have a BCA with ERC when previously the demarcation was the serial link?

- Please clarify how ERC is applied to standards when an SCI EACMS in a Medium Impact substation that provides conversion of ERC to serial for remote configuration support of RTU and Relays rated as Medium BCA along with Relays that are Low Impact BCA and Non-CIP System Relays how ERC is being applied when using serial communication has the proposed standard requirements intended that PSP and 15 month password changes now apply?

- Will applicability today for BCA with ERC apply going forward with the new proposed definitions and requirements to a BCS Medium Impact Relay connected serially that is being managed through RS-232?

- Does a Non-CIP System distribution Relay now become a PCA because it is connected to the Medium Impact Serial converter?

- The SDT ERC changes appears to be impacting the BROS process may require improved language in CIP-002 Attachment 1 as it cascades into other standards applicability requiring clarification:

  - CIP-002 R1 and R2 - Would Entities now need to identify BCA's that are serially connected and update CIP-002 BCS List to show these now as part of either SCADA or Protection with ERC?

  - CIP-004 R4.3 – Would electronic access to devices with ERC now be an entitlement to be mapped all serially connected devices requiring and role authorization?

  - CIP-005 R1.1 – Does the SDT expect that the ESP diagrams to now show serially connected devices within the substation house PSP and cables external out of the PSP to the devices in the structure including Transformers, CAP Banks, etc?

  - CIP-006 R1.2, 1.4, 1.7, 1.8, 1.9, 2.2, 2.3, 3.1 – Does the SDT intend that devices without ERC currently are outside a PSP (allowed by CIP-006 R1.1) will now with the proposed changes require the establishment of a PSP, with control, alerting, response, logging, visitor escort and system testing for serially connected IED in transformer cabinet for temperature monitoring, metering devices or other IEDs outside of the Station House PSP?

  - CIP-007 R1 – Please confirm the P1.1 Logical ports justification and details for serially connected CIP Systems are excluded but expectation of the physical wiring will be required for P1.2?

  - CIP-007 R4.2 – Please clarify the serial CIP System must now alert for failure of event logging.

  - CIP-007 R5.6 – Please clarify a serial CIP System such as an RTU or Relay that was a BCA or PCA without ERC now with the proposed change requires the password change every 15 months?

  - CIP-010 R1.1.4 – How will an Entity meet the baseline requirement for logical port open on each serially connected device or can a by device capability exclusion apply?

  - CIP-010 R1.2, 3, 4 – Do the proposed update require all the change management sub-requirements apply when a device is serially connected/disconnected to a network or moved within a network while still a serial device?

  - CIP-010 R3 – Please confirm the annual CVA including network discovery will require serial communication assessments throughout the site/facility/asset?

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No

Document Name	
Comment	
ACES does not agree with the reference “outside the asset containing” as a scoping mechanism for CIP-007 R4. We do not understand the correlation of ERC to CIP-007 logging or CIP-004 and CIP-006 risks. Using the “asset” as a scoping mechanism could lead to various interpretations and allow for loop holes for access. In our opinion, “outside the asset containing” is not necessary to define ERC. We feel ESP is still the proper scoping mechanism.	
Likes 0	
Dislikes 0	
Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	
Eversource recommends clarification regarding what "outside the asset containing" is clarifying.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA is concerned with bringing serial devices into scope as part of ‘Applicable System with ERC’. This would require the serial relays to comply with additional CIP requirements. Expanding the scope of ERC to serial-based devices could significantly increase implementation cost and require new tools/products to help with ensuring compliance. The changes needed to enforce Physical Security requirement CIP-006 R1.2 will require long lead times to implement especially for shared control houses.	
Likes 0	
Dislikes 0	
Response	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	

Answer	No
Document Name	
Comment	
<duplicate>	
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 agrees with the concept but does not agree with the proposed language. “Asset” should be better defined as it is too ambiguous and many requirements’ scoping is based on clarity around ERC. Additionally, ERC has changed from being defined in terms of a BCS to a ‘CIP System’ which includes all named types of devices. If a BCS inside an “asset” is isolated, however there is a docked TCA on another network inside the 'asset', does the BCS inherit ERC because a “CIP System” can be accessed in the asset? As the boundary broadens and the target is any CIP System, it has lost focus on the ability to externally communicate with a BCS. Southern suggests that ERC be defined in terms of the BCS, not the overly broad “CIP System”.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA is concerned with bringing serial devices into scope as part of ‘Applicable System with ERC’. This would require the serial relays to comply with additional CIP requirements. Expanding the scope of ERC to serial-based devices could significantly increase implementation cost and require new tools/products to help with ensuring compliance. The changes needed to enforce Physical Security requirement CIP-006 R1.2 will require long lead times to implement especially for shared control houses.	
Likes 0	
Dislikes 0	

Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT supports the IRC SRC comments and offers this additional comment: • The proposed modification greatly expands the scope of the definition. “Asset” has historically referred to things like transmission, generation, etc. Before, ERC was limited to just BES Cyber System. Why is this needed with assets and systems that reside outside of an ESP? The definition also needs to accommodate technologies that do not use a routable protocol.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
ATC supports the SDT’s intentions, however the proposed draft language is still somewhat unclear. For those reasons, ATC requests consideration of clearer language and perhaps supporting diagrams. One example of a question we’ve asked ourselves was: If you connect from a router (EACMS) to talk to a switch would that be ERC? Also, If my Control Center “asset” has several rooms and various subnets, and some devices are on a non-BCS subnet but still physically inside the “asset” containing the BCS, shouldn’t a routable connection from that device to a BCA be considered ERC?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not support the proposed change to the ERC definition because it expands the current definition by replacing the defined term BES Cyber System (BCS) with newly defined term “CIP System” and by changing from “... to access …” to “… to communicate …”. “Access” means the ability to	

make use of information (see NIST definition of access - https://csrc.nist.gov/glossary/term/access), while the term communicate has a much broader meaning and could be interpreted to mean that the act or ability to ping a device is now in scope.

Additionally, the use of the term “asset” within the context of the ERC definition raises potential compliance ambiguity and lack of uniformity that could result in different interpretations during an audit. To address these concerns, we offer the following:

The ability to access a BCS using a bidirectional routable protocol from outside the ESP that controls access to the BCS.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

This is a substantial change to the definition of ERC that has a larger impact than in the context of addressing virtualized environments.

This is a large change to bring into scope assets that are protected by the ESPs in the past but did not have to meet ERC requirement since this connection did not enable IRA.

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
The proposed change to the ERC definition expands scope by making the boundary physical “asset” from the original electronic concept. ERC could happen within a room where two systems have discrete ESPs that communicate between each other. Change the ability to “access” to “communicate to” to bring the connectivity rationale into the term. Suggested definition - *The ability to communicate to a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.*	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	

Answer	No
Document Name	

Comment

We understand that “outside the asset containing” is a scoping mechanism.

Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement?

We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary?

Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?

The overall definition of ERC is

The ability to communicate to a CIP System using a bi-directional routable protocol from outside the asset containing the CIP System.

(The definition of CIP System is included for precision)

The ability to communicate to a CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.) using a bi-directional routable protocol from outside the asset containing the CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.).

We don’t see the added value of this “scoping” for CIP-007 R4, CIP-004, CIP-006. This definition includes additional asset types (EACMS, PACS, SCI, PCA, TCA) to the concept of ERC. One could think that future requirements could come forward, like for EACMS with ERC or even TCA with ERC, but it’s not the case.

In reference to CIP-007 R4, the text used is the following

Medium Impact BCS with External Routable Connectivity and their associated:

1. EACMS;

2. PACS; and

3. PCA

SCI identified independently supporting an Applicable System above

The ERC trigger is still based on the BCS.

If the understanding of asset (“the asset containing “) is equivalent to the following … i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. RAS that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above… the suggested definition is interesting.

Our comprehension is that if we have two HIGH/Medium-Impact BCS in the same Control Center (asset) using a bi-directional routable protocol to establish their communication and that any of those BCS doesn’t use a bi-directional routable protocol outside of the Control Center, the ERC definition

wouldn't be applied. Furthermore, if any of those two BCS would be using a bi-directional routable protocol outside of the asset of both BCS would be tagged as being ERC.

We suggest the removal of CIP System in the definition.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

N&ST assumes this proposed revision is intended to bring into scope remote connections to serially-connected CIP Systems that traverse wide-area connections via TCP/IP before being converted, "locally," to serial. However, as written, it would exclude end-to-end routable connections from non-CIP Systems to CIP Systems established within a given asset (example: TCP/IP connection from a PC on corporate network to a CIP server in the same building behind an ESP on a CIP network). One loophole closed, another opened.

N&ST believes the SDT should be able to address this problem by expanding the definition of ERC using an "either/or" format. ERC is either:

"The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated ESP via a bi-directional routable protocol connection; or "The ability to communicate to a serially-connected CIP System using a bi-directional routable protocol from outside the asset containing the CIP System."

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	
Answer	No
Document Name	
Comment	

The IRC SRC understands “outside the asset containing” to be a scoping mechanism.

Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset and not the ESP. Is this understanding correct?

The IRC SRC is confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary?

Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. External Routable Connectivity (ERC) now means external to what?

Likes 0	
Dislikes 0	
Response	

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	
Response	

Dan Zollner - Portland General Electric Co. - 3	
Answer	No
Document Name	
Comment	

Portland General Electric Company supports the comments provided by EEI for this survey question.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Dominion Energy agrees with the reason for the reference “outside the asset containing…” but the definition itself does not help determine if ERC exists within a communication link that involves a routable protocol that is converted to serial protocol at the last leg of the link. However, based on the NERC SDT Webinar, presented on August 4, it appears that ERC exists in this kind of communication. One or more high level reference diagrams that illustrate the general concept of the modified term ERC, or some examples of the concept, in an Implementation Guidance document would be beneficial. See also response to #14A below.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	Yes
Document Name	

Comment

Chelan agrees with the proposed definition changes for ERC.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	Yes
Document Name	

Comment

As long as ERC is not used instead of IRA. PNMR supports EEIs suggested definition of ERC.

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE does not have MEDIUM impact BCS cases and thus no cases for which the ERC definition would affect scope for requirements.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Agree with change to ERC definition.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
While GSOC agrees with the intent of the change, it cannot support the proposed change as use of the generic term “asset” could cause confusion and inconsistency regarding the meaning of the term “asset” and its use across the body of standards. As an example, asset is utilized in CIP-002 and is meant to convey a physical facility or building. The generic use of “asset” within the new definition of ERC could, therefore, also be construed as referring to the physical building or facility in which a system is located, which is likely not the intended or	

only meaning. To reduce the potential for confusion, GSOC recommends that clarification be added to the definition of 'ERC' to ensure that the full intent and meaning of the term "asset" as used within the definition of ERC is clear and easily, consistently understood.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Yes, we argree with the proposed change because the language "through an EACMS controlling communications..." allows non-peri meter-based models of ERC including zero-trust.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
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	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

N&ST believes the “routable protocol” qualifier should be retained:

“A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.”

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	

Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

We suggest adding “routable protocol” to the revised definition. We feel this can still be used for both types of networks. We also suggest removing “CIP Systems,”and replace with “BES Cyber Systems.” Remove “enforced by an EACMS.”

Suggested definition - *A set of configurations or policies [delete - enforced by an EACMS] that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber Systems of the same impact rating and their associated PCA.*

Likes 0	
Dislikes 0	
Response	

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI agrees that the modified ESP definition can be used for both types of networks but seeks clarification regarding the inclusion of the phrase “and their associated PCAs”, which appears to be redundant to the second sentence in the definition. EEI notes that within the definition of CIP System, PCAs are clearly identified as a CIP System. We suggest the following as one possible solution:

“A set of configurations or policies enforced by an EACMS that control routable protocol communications to or from any part of a BES Cyber System (BCS) and that groups BCS of the same impact rating.”

Alternatively, the SDT might consider leveraging the defined term “Electronic Access Point (EAP)” rather than modifying the term ESP.

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

The phrase "control communication" is too broad; it could include any policy/configuration that configures anything that communicates (e.g., an internal API within an application). The definition needs additional clarity such that an ESP is in the networking realm and is controlling the ability to deliver packets to a BCS on the network, which we gather is the intent since host-based firewalls are excluded. We suggest modifying it to "control routable protocol communication" to clarify that an ESP is a network level construct (even in zero trust) concerned with delivery of packets.

The grouping statement in the ESP definition is confusing as it switches to "CIP Systems" and only BCS have impact ratings. Suggest changing this to "These configurations or policies group BES Cyber Systems of the same impact rating with their associated PCAs". In addition, we believe this sentence is attempting to say the ESP is the ‘innermost’ policy or configuration controlling access to the BCS and therefore grouping BCS of like impact rating and their PCAs. We suggest making further clarifications to that end. An enterprise’s Internet facing firewalls play some role in ‘controlling communications’ to eventual groups of BCS that may be many network zones deep behind many firewalls that are not the CIP-005 ESP of today. However, there appears to be nothing in the definition or CIP-005 R1.1 that clearly states the ESP in question is the layer of segmentation/isolation method immediately ‘outside’ the BCS.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	No
Document Name	

Comment

The SDT is using the update to the definition as a mechanism to support zero-trust models, but the existing ESP definition does not preclude a Responsible Entity from applying the concept of zero-trust to its environment(s) in addition to its traditional ESP. The proposed modification does not obligate a Responsible Entity to adopt additional security controls.

The statement in the Definitions and Exemptions Technical Rationale, “[i]n these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS and nothing on the network is trusted for unrestricted communications,” could be

interpreted as meaning that traditional ESP-based perimeter security is not necessary or required. A Responsible Entity may choose to adopt a traditional ESP model, or a zero-trust model, without considering the benefits of a defense-in-depth approach that leverages both traditional perimeter-based security and zero-trust concepts.

AWS proposes the following language, “The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol that includes a set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.”

Detailed implementation guidance is necessary to support zero-trust and hybrid approaches.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No

Document Name	

Comment

Relative to the definition of ESP, GSOC is concerned that the second sentence proposed in the new definition is unnecessary and could cause confusion regarding its applicability beyond a virtualized environment. In particular, use of the term "group" could connote actions or protections beyond the traditional and intended meaning of ESP. As well, the second sentence appears to act as an additional requirement on the use of ESPs that would be better suited for inclusion in the actual requirements as set forth in CIP-005-8. GSOC recommends deleting the second sentence from the definition and re-capturing the concept (as applicable) in the language of CIP-005-8.

GSOC requests the addition of clarifying language in CIP-005-8 R1.2 that would reinforce the approach of utilizing a traditional approach to electronic security perimeters in addition to the language proposed "EACMS that enforces an ESP for the Applicable System…" Current proposed language could be interpreted to only apply to communications traversing an EACMS enforcing an ESP in a virtualized environment, without providing for requirements concerning the same traffic traversing a traditional ESP such as a firewall or similar device.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The modified ESP definition does not resolve the traditional firewall based network or future networks. The virtualization zero trust topology is underneath the ESP network and is a non-ESP model. It is configured in the virtualization layer prior to VCAs reaching the ESP network. IRA cannot be identified without an ESP boundary being defined since IRA is initiated outside ESP. Furthermore, the SDT proposed ESP definition would include routable and non-routable BCAs in which it overreaches the goal of SAR. In our view, the EAP is still effective for the ESP model to control communications to and from BCS using routable protocol inside an ESP. We recommend adding an alternative requirement in CIP-005 R1.1 to address the zero-trust model in which the ESP model is not used rather than revising ESP definition. Our proposed changes won't affect the existing ESP definition and ESP related requirements while still addressing virtualization to meet the goal of SAR.

Recommendations:

1. Restore the current ESP definition since it is still effective for the perimeter-based routable network protection.
2. We propose the following changes for CIP-005 R1.1:

    i. All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP where all External Routable Connectivity must be through an identified EAP that permits only needed inbound and outbound access and denies all other access by default including the reason for granting access, or

    ii. All BCAs connected to a network via a routable external protocol shall through an EACMS that controls all communications to and from BCAs unless ESP model is used.

    We agree that the proposed ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. However, the routable protocol qualifier was removed and the new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. This seems like a circular definition. Also, it is our

understanding that the SDT does not intend to have requirements baked into definitions but with the proposed ESP definition, and changes to CIP-005, the definition is the only place EACMS are required. We propose the following changes:

ESP definition: A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

New CIP-005-X R1 Part 1.X:

Applicable Systems

High Impact BES Cyber Systems and their associated PCA

Medium Impact BES Cyber Systems and their associated PCA

Requirements

1.X.1 - EACMSs must be implemented to enforce ESPs where communication leaves the ESP, or where SCI is used.

1.X.2 - EAPs must be identified for ESPs.

When the proposed ESP definition is applied in the proposed CIP-005-X R1 Part 1.1 there is another issue since the definition no longer has the routable protocol qualifier. See our response to Question #10 below for further explanation.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

In our opinion it should be clarified that a BCA or PCA controlling access only to itself (such as a host-based firewall) does not qualify as an EACMS and likewise does not constitue an ESP, except in cases where zero-trust is being used in place of a traditional EACMS and Access Point (such as a firewall). We also support EEI's comments on this question.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
Suggesting that the SD go back and make modifications to the definitions. We agree that the proposed ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. However, the routable protocol qualifier was removed and the new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. This seems like a circular definition. Also, it is our understanding that the SDT does not intend to have requirements baked into definitions but with the proposed ESP definition, and changes to CIP-005, the definition is the only place EACMS are required. We propose the following changes: ESP definition: A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs. New CIP-005-X R1 Part 1.X: Applicable Systems High Impact BES Cyber Systems and their associated PCA Medium Impact BES Cyber Systems and their associated PCA Requirements 1.X.1 - EACMSs must be implemented to enforce ESPs where communication leaves the ESP, or where SCI is used. 1.X.2 - EAPs must be identified for ESPs. When the proposed ESP definition is applied in the proposed CIP-005-X R1 Part 1.1 there is another issue since the definition no longer has the routable protocol qualifier.

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	No
Document Name	

Comment
We suggest adding “routable protocol” to the revised definition. We feel this can still be used for both types of networks. We also suggest removing “CIP Systems,” and replace with “BES Cyber Systems.” Remove “enforced by an EACMS.” Suggested definition - *A set of configurations or policies [delete - enforced by an EACMS] that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber Systems of the same impact rating and their associated PCA.*

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3	
Answer	No
Document Name	
Comment	
GRE agrees with the comments submitted by the NSRF.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
While the modified ESP definition is a definite improvement with respect to support for future development of zero trust networking adoption, the measures associated with proposed CIP-005-8 R1 include specification of business reasons associated with the configuration identified in the definition. ISO-NE requests that the definition be updated to include the business reasons as a part of the ESP to clarify the relationship and the requirement to include such in the configuration and documentation related to ESP's.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We suggest adding “routable protocol” to the revised definition. We feel this can still be used for both types of networks. We also suggest removing “CIP Systems,”and replace with “BES Cyber Systems.” Remove “enforced by an EACMS.” Suggested definition - *A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber Systems of the same impact rating and their associated PCA.*	
Likes 0	

Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We disagree with the modified ESP definition as it cannot resolve the traditional firewall based network and the future networks. The virtualization zero trust topology is underneath the ESP network and is a non-ESP model. It is configured in the virtualization layer prior to VCAs reaching the ESP network. Also, IRA cannot be identified without ESP boundary being defined since IRA is initiated outside ESP. Furthermore, the SDT proposed ESP definition would include routable and non-routable BCAs in which it overreaches the goal of SAR. In our view, the EAP is still effective for the ESP model to control communications to and from BCS using routable protocol inside an ESP. We recommend adding an alternative requirement in CIP-005	

R1.1 to address the zero-trust model in which the ESP model is not used rather than revising ESP definition. Our proposed changes won't affect the existing ESP definition and ESP related requirements while still addressing virtualization to meet the goal of SAR.

Recommendations:

1. Restore the current ESP definition since it is still effective for the perimeter-based routable network protection.

2. We propose the following changes for CIP-005 R1.1:

a. All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP where all External Routable Connectivity must be through an identified EAP that permits only needed inbound and outbound access and denies all other access by default including the reason for granting access, or

b. All BCAs connected to a network via a routable protocol shall through an EACMS that controls all communications to and from BCAs unless ESP model is used.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

While AEP agrees that the modified Electronic Security Perimeter (ESP) definition can be used for both type of networks (i.e., traditional firewall based networks, as well as future networks such as zero trust), we recommend the second sentence be removed. The second sentence, "These configurations or policies group CIP Systems of the same impact rating and their associated PCAs", seems to be an arbitrary statement that does not build upon the security requirement. A semantic argument could be made that once the configurations or policies are established, all CIP Systems inherit the highest water mark; however, prior to the establishment, the inherent risk of the associated CIP Systems could differ. We suggest removing the second sentence to avoid future confusive discussion.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

We suggest adding “routable protocol” to the revised definition. We feel this can still be used for both types of networks. We also suggest removing “CIP Systems,”and replace with “BES Cyber Systems.” Remove “enforced by an EACMS.”

Suggested definition - *A set of configurations or policies (**Remove: enforced by an EACMS)** that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber Systems of the same impact rating and their associated PCA.*	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

Although the revised definition allows for both traditional firewall-based networks as well as more modern protections, the definition remains incomplete. We would suggest altering the definition as follows: "**A logical boundary defined by** a set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System and that groups CIP Systems of the same **or lower** impact rating"

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	No
Document Name	

Comment

MEAG Power adopts the Southern Commany comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The proposed change ignores the concept of an isolated ESP network and instead requires an EACMS be deployed regardless to control communications between BCS, PCAs within the same network. The application of an EACMS in an isolated ESP network would add no extra protections or benefit for the purpose of controlling communications within the network given there are no Electronic Access Points applicable in relation to routable traffic from outside of the ESP or exiting the ESP.

BC Hydro recommends clarifying that the EACMS requirement portion of the definition be applicable only in cases where ERC may exist (i.e. discrete ESPs or extended ESPs).

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	
New ESP definition would disallow including assets of lower impact ratings in a higher security environment, thus preventing the potential implementation of security best practices on Medium or Low impact assets. The new definition of ESP would also prevent the use of VLANs as a method of demonstrating isolation of BCS and other Cyber Assets as the Switches involved with managing of VLANs are often classified as BCAs and under the current CIP standards an asset classified as a BCA cannot be classified also as an EACMS, PCA or PACS.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
The second sentence appears to be redundant due to the phrase “and their associated PCAs” since PCAs are included within the proposed “CIP System” definition. SIGE proposes the following: “A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System and that groups CIP Systems of the same impact rating.”	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	

NCPA supports most of the definition change, however “policies” are a vague reference. NCPA proposes using the phrase “technical policies” as to not confuse them with administrative policies.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

The second sentence appears to be redundant due to the phrase “and their associated PCAs” since PCAs are included within the proposed “CIP System” definition. CEHE proposes the following:

“A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System and that groups CIP Systems of the same impact rating.”

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	

Comment

There is no clear point of demarcation where the border of the ESP is defined, introducing significant concerns how the boundary of the CIP standard will be evaluated and enforced. Recommend retaining current definition. While not necessary, it may be appropriate to clarify that additional controls may be implemented within the security perimeter to limit communication ports inside of requirement CIP-007 R1.1

Likes 0	
Dislikes 0	

Response

Josh Johnson - Lincoln Electric System - 1

Answer	No

Document Name	

Comment

While we do not believe it to be the intent of the SDT, we disagree with the new definition(s) of EACMS and ESP as it is less clear what is and is not considered an ESP. Currently, a substation facility BCS that is not utilizing routable protocols, such as an RTU serially connected to several relays, is not classified as an ESP and subsequently, the RTU (which could be used as a central access point to the relays) would not be classified as an EACMS. This clarity is lost with the proposed definition changes.

Recommendation:

Electronic Security Perimeter (ESP) – The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or

A set of configurations or policies enforced by an EACMS that controls routable communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Electronic Access Control or Monitoring Systems (EACMS) – Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring via routable protocols of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems and SCI grouped by the Responsible Entity, in the EACMS it supports.

Likes 0	
Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5

Answer	No
Document Name	

Comment

We agree that the proposed ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. However, the routable protocol qualifier was removed and the new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. This seems like a circular definition. Also, it is our understanding that the SDT does not intend to have requirements baked into definitions but with the proposed ESP definition, and changes to CIP-005, the definition is the only place EACMS are required. We propose the following changes:

ESP definition: A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

New CIP-005-X R1 Part 1.X:

Applicable Systems

High Impact BES Cyber Systems and their associated PCA

Medium Impact BES Cyber Systems and their associated PCA

Requirements

1.X.1 - EACMSs must be implemented to enforce ESPs where communication leaves the ESP, or where SCI is used.

1.X.2 - EAPs must be identified for ESPs.

When the proposed ESP definition is applied in the proposed CIP-005-X R1 Part 1.1 there is another issue since the definition no longer has the routable protocol qualifier. See our response to Question #10 below for further explanation.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	No
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Duke Energy agrees with the directional change but has identified several concerns with the proposed language.

First, the use of CIP Systems in the definition is in conflict with the use of BES Cyber System as the initial scoping in the definition, as it could be interpreted to require ESPs around EACMS and PACS that are outside the traditional ESP boundary on separate hardware. Further, this introduces a redundancy between the CIP Systems and PCA definitions.

Second, the use of the term policies is ambiguous in context and is likely to be conflicted with written policies (e.g. procedurally requiring password rotation). Policy-based access control is configured into the enforcing system, and therefore is inherently included in the configuration term. This should be made explicit in measures or guidance documents to ensure the intent to allow future policy-based access control is apparent.

Third, the inclusion of qualifiers to address the host-based firewall concern in the requirement language is inappropriate as it addresses specific solutions. A better means of addressing this concern would be to include qualifiers in the definition of ESP to ensure that the configurations enforcing the perimeter do not reside on a BES Cyber Asset.

DUKE ENERGY PROPOSED DEFINITION FOR ESP:

A set of configurations enforced by an EACMS that creates a logical boundary where communications to or from any part of a BES Cyber System and any PCA or SCIG associated with a BES Cyber System are controlled. All BCS, PCA, and SCIG included in an ESP have the same impact rating as the highest included device. The EACMS enforcing the ESP may not be part of a BES Cyber System.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

BPA agrees that the modified definition is more flexible for future ESPs using a zero trust environment. However, additional language is needed to address whether the SDT still intends for standalone networks that have no external connectivity to other networks (”standalone networks”) to have a defined ESP.

Option 1: If standalone networks DO NOT require an ESP, please update the Technical Rationale to address standalone networks (as was traditionally done in the TR for CIP-005-6 and CIP-005-7).

Option 2: If standalone networks DO still require an ESP, the proposed definition requires all ESPs to be “enforced by an EACMS;” this will add a high burden for standalone networks. For example, a standalone ESP consisting of a local operator HMI (PCA, used for local review of SCADA alarms) connected to 2 local SCADA RTUs (BCAs) via a switch (PCA) would need to have an EACMS added in order to meet the letter of the requirement, but without gaining any security or protection.

Option 2 proposed language: move the “enforced by an EACMS” from the definition of an ESP, to a new requirement for BCS with ERC:

(1) Definition for Electronic Security Perimeter (ESP): A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Benefit: This would permit the isolated nature – or “configuration” – of the small local network to provide the control of communications to/from the BES Cyber System by simply excluding it.

(2) Add an additional requirement under CIP-005-8 R1.1 [hypothetically referenced here as R “1.1-A” for numbering clarity] for the EACMS portion:

Requirement: 1.1-A

Applicable Systems: BCS with ERC and their associated PCA Requirements: Utilize an EACMS to enforce the control of communications to or from any part of a BES Cyber System.

(3) Related update is needed to correct the Applicable Systems in R2.1: “EACMS that enforces an ESP for the Applicable Systems in Part 1.1-A.”

(4) Update the Technical Rationale (TR) to clarify for standalone networks (as was traditionally done in the **TR for CIP-005-6 and CIP-005-7**).

Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
While the term ESP was restored, the definition shifted to a logical format much like ACLs while referencing the physical ESP with the definition of IRA Suggest clarify definition of ESP and IRA.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
The proposed change to the ESP definition adds a significant amount of ambiguity. Within the context of the new definition, the term “Electronic Security Perimeter” doesn’t seem to apply. ESP references a “perimeter” and the definition doesn’t indicate a logical perimeter of any sort. If anything, the definition essentially becomes synonymous only with the policies or rulesets mandated by a firewall. NRG recommends reverting the ESP term back to its original definition.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
The proposed change to the ESP definition adds a significant amount of ambiguity. Within the context of the new definition, the term “Electronic Security Perimeter” doesn’t seem to apply. ESP references a “perimeter” and the definition doesn’t indicate a logical perimeter of any sort. If anything,	

the definition essentially becomes synonymous only with the policies or rulesets mandated by a firewall. NRG recommends reverting the ESP term back to its original definition.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	
Answer	Yes
Document Name	
Comment	
The IRC SRC agrees that the proposed change to the ESP definition supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.”	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.” The new definition can be used for both traditional firewall-based networks, as well as future networks such as zero-trust but we don’t agree on the overall definition. The suggested definition broadens the current scope, it implies the presence of an EACMS, thus requesting another cyber asset (We have a BCA: VCA and we have an EACMS: Firewall) unless the SDT wanted to permit the double categorization (BCA/EACMS: a VCA with an embedded firewall) The language “that controls communications” isn’t consistent with the NERC CIP orientation, usage of the bi-directional routable protocol should be used because with the current language one could imply that serial, layer 2 communication needs to have a set of configurations or policies. Also, the definition states that this is for a BES Cyber System (…any part of a BES Cyber System…), yet the definition mention CIP System (… policies group CIP Systems of the same …). The definition of CIP System includes more than BES Cyber System. We suggest reviewing the definition.	

The proposal could be

A set of configurations or policies enforced those controls bi-directional routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber System of the same impact rating and their associated PCAs.

Reference: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	Yes
Document Name	

Comment

PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

ERCOT supports the IRC SRC comments.

Likes 0	
Dislikes 0	

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer	Yes

Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	Yes
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
The new ESP may be logical/virtual or physical boundary applied using firewalls and zero trust.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

We agree that the proposed ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

In support of IRC SRC/SWG.

We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	Yes
Document Name	

Comment

Suggest the following modification to the ESP definition:

“These configurations or policies ***protect a*** group of CIP Systems of the same impact rating and their associated PCAs.”

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment
We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.” The new definition can be used for both traditional firewall-based networks, as well as future networks such as zero-trust but we don’t agree on the overall definition. The suggested definition broadens the current scope, it implies the presence of an EACMS, thus requesting another cyber asset (We have a BCA: VCA and we have an EACMS: Firewall) unless the SDT wanted to permit the double categorization (BCA/EACMS: a VCA with an embedded firewall) The language “that controls communications” isn’t consistent with the NERC CIP orientation, usage of the bi-directional routable protocol should be used because with the current language one could imply that serial, layer 2 communication needs to have a set of configurations or policies. Also, the definition states that this is for a BES Cyber System (…any part of a BES Cyber System…), yet the definition mention CIP System (… policies group CIP Systems of the same …). The definition of CIP System includes more than BES Cyber System. We suggest reviewing the definition. The proposal could be A set of configurations or policies enforced those controls bi-directional routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber System of the same impact rating and their associated PCAs. Reference: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	

Comment
In support of NPCC RSC comments. We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.” The new definition can be used for both traditional firewall-based networks, as well as future networks such as zero-trust but we don’t agree on the overall definition.

The suggested definition broadens the current scope, it implies the presence of an EACMS, thus requesting another cyber asset (We have a BCA: VCA and we have an EACMS: Firewall) unless the SDT wanted to permit the double categorization (BCA/EACMS: a VCA with an embedded firewall)

The language “that controls communications” isn’t consistent with the NERC CIP orientation, usage of the bi-directional routable protocol should be used because with the current language one could imply that serial, layer 2 communication needs to have a set of configurations or policies.

Also, the definition states that this is for a BES Cyber System (…any part of a BES Cyber System…), yet the definition mention CIP System (… policies group CIP Systems of the same …). The definition of CIP System includes more than BES Cyber System.

We suggest reviewing the definition.

The proposal could be

A set of configurations or policies enforced those controls bi-directional routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber System of the same impact rating and their associated PCAs.

Reference: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	Yes
Document Name	

Comment

We support NPCC TFIST's comments as found below:

We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	Yes
Document Name	

Comment

SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the modified ESP definition can be used for both traditional and future networks. However, the inclusion of the phrase “and their associated PCAs” is redundant and unnecessary since CIP Systems include associated PCAs by definition.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
The first sentence alone in the ESP definition seems to be able to be used for both traditional firewall-based networks and future networks. The second sentence is confusing in that a CIP System would have an associated PCA when PCA is already part of the CIP System definition.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Chelan agrees with the proposed definition changes for ESP.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
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	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

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

Texas RE agrees with the proposed definition of ESP. The SDT could, however, consider revision it to the following for clarification:

- A boundary of protection set by configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs

Texas RE does note, however, that the proposed change to CIP-005 R1.1 explicitly states that host-based firewalls that only protect the host on which they reside are not a sufficient control to meet compliance with the requirement. Mass deployment of host-based firewalls is one method by which an organization can work toward implementing a zero-trust security model. The SDT may wish to consider this in the evaluation of its proposed ESP definition.

Likes 0	
Dislikes 0	
Response	

5. The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

The new IRA definition could expand scope significantly. For instance, the second bullet within the proposed IRA definition – "through a Cyber Asset or Virtual Cyber Asset that is convering communications…" – could potentially bring into scope an operator at a Control Center increasing megawatts at a Medium without ERC plant and classify that scenario as IRA.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

The new IRA definition could expand scope significantly. For instance, the second bullet within the proposed IRA definition – "through a Cyber Asset or Virtual Cyber Asset that is convering communications…" – could potentially bring into scope an operator at a Control Center increasing megawatts at a Medium without ERC plant and classify that scenario as IRA.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

There is insufficient clarity provided within the proposed terms to ensure consistent understanding and identification of applicable traffic.

Likes 0	

Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Suggest removing ‘Responsible Entity’s’ as it should still be considered IRA if a user at one entity, outside an ESP, connected remotely to another entity's ESP. Additionally, consider changing ‘person’ to Cyber Asset. The use of a person in the context being ‘outside an Electronic Security Perimeter’ does not make sense. Suggest the following - User-initiated real-time access from a Cyber Asset outside of the Electronic Security Perimeters (ESP) using a routable protocol: Bullets one and two are in the singular tense, consider changing bullets three and four from plural tense to single tense as well. Bullet three to – ‘To a Management Interface of a Shared Cyber Infrastructure; or’ and bullet four to – ‘To a Management Interface of an Electronic Access Control or Monitoring System that enforces an ESP.’	

Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
The use of ‘within an ESP’ doesn’t work with the new ESP definition. Alternative proposal: Replace ‘from outside of the Responsible Entity’s Electronic Security Perimeters’ with ‘from a Cyber Asset that is not protected by an Entity’s Electronic Security Perimeters’, and replace ‘within an ESP’ and ‘within an Electronic Security Perimeter’ with ‘protected by an Electronic Security Perimeter’. Additionally, focusing on Mangement Interfaces rather than SCI itself could allow access to the SCI through an additional port that doesn’t meet the definition of a Management Interface.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
This definition introduces significant ambiguity and would rely excessively on non-enforcable Technical rationales and guidelines. As a result, it is subject to significant ambiguity. This ambiguity is further increased by the change in the definition of ESP that removes a clearly defined border of the ESP.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	

The second bullet point is not clear. Need for clarification

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

The definition of 'IRA' is unclear on the overall impact to the current infrastructure. Please further clarify as the second bullet "through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;" suggests that non-CIP devices will fall under the purview of this definition with the use of the NERC-defined term "Cyber System" being contained within the above language

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE does not agree with the proposed changes to the Interactive Remote Access definition because it seems to be unnecessarily confusing due to unneeded information within the definition.

The first bullet “to a Cyber System within an ESP” covers access to any Cyber System including its user interface ports. Therefore it is unnecessary to have the third and fourth bullet items. The third bullet specifies Management Interfaces of SCI, and similarly the fourth bullet specifies the Management Interfaces of the EACMS that enforces an ESP. However both SCI and EACMS are Cyber Systems which are covered by the first bullet.

The purpose of the fourth bullet is to capture remote access through a “serial to IP” device, and to achieve this the bullet item goes through a complex explanation on the conversion of routable to non-routable communications and Cyber Systems not in an ESP. The same thing can be accomplished by removing the phrase “using a routable protocol” from the first part of the definition. Then, to capture Cyber Systems not within an ESP, it seems that including “… Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) …” would more clearly capture this.

In addition, CEHE understands that a cabinet can be a PSP, and someone standing outside of the cabinet and physically connecting to a system within a cabinet is not IRA. This situation is not a remote connection therefore is not IRA and may need to be explained in the technical rationale.

IRA should not be prescribed to only “a routable protocol”. It should include all methods by which this is accomplished, even by a dial-up connection. However, CIP-005-8 requirement R2 specifically excludes Dial-up Connectivity. This is how the process should work. The definition states what IRA is, and the requirements specify exactly what applies.

Based upon those thoughts CEHE proposes the following:

“A user initiated real-time electronic access by a person from outside of a Responsible Entity’s Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) to a CIP System within the Responsible Entity’s ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System’s user interfaces.”

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)

Answer	No
Document Name	

Comment

Comments:

Clarification is needed around the Management Interfaces of a Shared Cyber Infrastructure (SCI). Is the intent to limit the definition of Management Interfaces that manage SCI and the other bulleted items in the definition, or is the intent to include all Management Interfaces?

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree with the proposed changes to the Interactive Remote Access definition because it seems to be unnecessarily confusing due to unneeded information within the definition.

The first bullet “to a Cyber System within an ESP” covers access to any Cyber System including its user interface ports. Therefore it is unnecessary to have the third and fourth bullet items. The third bullet specifies Management Interfaces of SCI, and similarly the fourth bullet specifies the Management Interfaces of the EACMS that enforces an ESP. However both SCI and EACMS are Cyber Systems which are covered by the first bullet.

The purpose of the fourth bullet is to capture remote access through a “serial to IP” device, and to achieve this the bullet item goes through a complex explanation on the conversion of routable to non-routable communications and Cyber Systems not in an ESP. The same thing can be accomplished by

removing the phrase “using a routable protocol” from the first part of the definition. Then, to capture Cyber Systems not within an ESP, it seems that including “… Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) …” would more clearly capture this.

In addition, SIGE understands that a cabinet can be a PSP, and someone standing outside of the cabinet and physically connecting to a system within a cabinet is not IRA. This situation is not a remote connection therefore is not IRA and may need to be explained in the technical rationale.

IRA should not be prescribed to only “a routable protocol”. It should include all methods by which this is accomplished, even by a dial-up connection. However, CIP-005-8 requirement R2 specifically excludes Dial-up Connectivity. This is how the process should work. The definition states what IRA is, and the requirements specify exactly what applies.

Based upon those thoughts SIGE proposes the following:

“A user initiated real-time electronic access by a person from outside of a Responsible Entity’s Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) to a CIP System within the Responsible Entity’s ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System’s user interfaces.”

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

The definition states that the communication is to a system within an ESP, but the last bullet states that IRA applies to Management Interfaces for EACMS that enforce an ESP. The problem with this is that the Management Interface does not necessarily reside within the ESP.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE is concerned with the use of the term “real-time” as it is a defined word in the NERC Glossary. This could introduce confusion. Texas RE recommends removing this term from the language.

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an	

Electronic Security Perimeter;" to "to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;".	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
As written and presented, there is a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication, but have not adequately enforced protections to ensure that the ports are not used by malicious actors regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to ensure validity of communications to Applicable Systems. In addition, approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization and approval of SCI terminology and other definitions associated with virtualization as a whole.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	

Comment
The definition needs clarification that system-to-system communications are not considered IRA. Add the following sentence back to the end of the definition as with the currently approved definition: “Interactive Remote Access does not include system-to-system process communications.”

Likes 0	
Dislikes 0	

Response

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

Comment
See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	

Comment
Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;” to “to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;”.

The new definition of ESP mentions an ESP is a …set of configurations or policies enforced by an EACMS… This definition doesn’t establish a boundary (logical border) so the language outside of the Responsible Entity’s Electronic Security Perimeters (ESP) or within an ESP doesn’t work.

The introduction of the converting functionality is interesting.

We suggest reviewing the definition of ESP/IRA/EAP.

Alternate proposal

User-initiated real-time access by a person outside of BES Cyber System, using a routable protocol:

• to a BES Cyber System;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a BES Cyber System

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Reference

User-initiated real-time access by a person from outside of the Responsible Entity’s Electronic Security Perimeters (ESP). using a routable protocol:

• to a Cyber System within an ESP;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6	
Answer	No
Document Name	

Comment
AEP believes additional clarity is needed to the proposed definition of Interactive Remote Access (IRA) and provides the following revised introduction sentence for consideration. *"A user initiated electronic access by a person from outside of a Responsible Entity's Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP) using a routable protocol to a CIP System within the Responsible Entity's ESP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System's user interfaces. This includes access to:* • *Cyber Systems within an ESP;* • *Through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter*; • *To Management Interfaces of a Shared Cyber Infrastructure; or* • *To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP"* We suggest "real-time" be stricken from the definition as we believe there is no function that would allow "a person" to interact with a system in any frame of time other than "real-time". While we recognize the attempt to establish that this would not include batch processing, it is our opinion that the batch would run system-to-system and would not qualify as "a person".

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	

Comment
We agree with the changes if real-time is being used as the NERC defined word. If that was the intent, it should be capitalized. If not, there should be more clarification around what real-time is. We agree if the intent is to continue to exclude system to system process communications.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment

Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;” to “to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;”.

The new definition of ESP mentions an ESP is a …set of configurations or policies enforced by an EACMS… This definition doesn’t establish a boundary (logical border) so the language outside of the Responsible Entity’s Electronic Security Perimeters (ESP) or within an ESP doesn’t work.

The introduction of the converting functionality is interesting.

We suggest reviewing the definition of ESP/IRA/EAP.

Alternate proposal

User-initiated real-time access by a person outside of BES Cyber System, using a routable protocol:

• to a BES Cyber System;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a BES Cyber System

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Reference

User-initiated real-time access by a person from outside of the Responsible Entity’s Electronic Security Perimeters (ESP). using a routable protocol:

• to a Cyber System within an ESP;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We disagree with the proposed changes because much of the existing IRA definition is clear and effective. The SDT should only clarify whether the entire communication path needs to be routable from the remote client to the end device.

Recommendation: We recommend making a minor change to the existing IRA to clarify the concept of a routable protocol converting to non-routable so that it can meet the goal of the SAR. (See our proposed changes to IRA and rationale in Q1

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

Third bullet should read “To Management Interfaces of an Shared Cyber Infrastructure ***within*** *an ESP*; or” unless the SDT is trying to bring IRA restrictions to devices outside an ESP. In which case the applicability should be expanded further.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

The definition needs clarification that system-to-system communications are not considered IRA. Add the following sentence back to the end of the definition as with the currently approved definition: “Interactive Remote Access does not include system-to-system process communications.”

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;” to “to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;”.

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	No
Document Name	

Comment

The definition needs clarification that system-to-system communications are not considered IRA. Add the following sentence back to the end of the definition as with the currently approved definition: “Interactive Remote Access does not include system-to-system process communications.”

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment
We are concerned with the implications of these changes in conjunction with the changes in definition to ESP, EACMS, and the addition of serial communication. To avoid confussin we believe this needs to be clarified within CIP-005 that CIP-005 IRA requirements do not apply to BCAs or PCAs controlling access only to themselves (such as host-based firewalls) when a traditional EACMS and Access Point (such as a site firewall) is being used.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	

Comment
We disagree with the proposed changes because much of the existing IRA definition is clear and effective. The SDT should only clarify whether the entire communication path needs to be routable from the remote client to the end device. **Recommendation:** We recommend making a minor change to the existing IRA to clarify the concept of a routable protocol converting to non-routable so that it can meet the goal of the SAR. (See our proposed changes to IRA and rationale in Q1.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	

Comment
• IRA with ERC has been confusing for Entities to understand when the conversion to serial devices appears to now be in scope if configurations may be impacted using serial thus requiring, for example password changes within 15 months.   ○ Please provide more examples including transitioning BCA currently without ERC when it becomes BCA with ERC under the new proposed definitions and standards. How and where is the change applied and if it will be part of CIP-002? • Does a Non-CIP System distribution Relay now become a PCA because it is connected to the Medium Impact Serial converter if it supports IRA?

Likes 0	

Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	
<duplicate>	
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 changes concerning clarity for IP-serial conversions, but does not support the changes for Management Interfaces such as those on an “EACMS that enforces an ESP”. An Intermediate System is an EACMS that helps enforce an ESP which could open up a “Hall of Mirrors” scenario where an Intermediate System is required to access an Intermediate System. This hall of mirrors is stated in the Applicable Systems column of CIP-005 R2.1 (in the clean version of CIP-005 that was posted, which differs from the redline).	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT supports the IRC SRC comments and offers these additional comments: • Bullet 2: This appears to be backwards. It reads like you are sending communications outside the ESP. • Bullet 3: Please clarify if “To Management Interfaces of a Shared Cyber Infrastructure” is only related to the Cyber Assets within the ESP. • Bullet 4: Adding “To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforces an ESP” expands the scope of the existing definition by protecting more than just what resides inside the ESP.	
Likes 0	

Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Comments: EEI asks for additional clarity for the proposed definition of IRA. It is unclear why the definition includes “real-time” when the proposed definition specifically applies to access by a person. If “real-time” was inserted for a specific purpose, then the SDT should provide a clear explanation. Additionally, if “real-time” is needed, EEI recommends that the definition also include “IRA does not include system to system process communications or read-only access.”

“A user initiated real-time electronic access by a person from outside of a Responsible Entity’s Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) using a routable protocol to a CIP System within the Responsible Entity’s ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System’s user interfaces. This includes access to:

1. *Cyber Systems within an ESP;*
2. *Through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;*
3. *To Management Interfaces of a Shared Cyber Infrastructure; or*
4. *To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP”*
5. ***IRA does not include system to system process communications or read only access**.*

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
The definition needs clarification that system-to-system communications are not considered IRA. Add the following sentence back to the end of the definition as with the currently approved definition: “Interactive Remote Access does not include system-to-system process communications.”	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	

Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	

Comment
Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;” to “to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;”. The new definition of ESP mentions an ESP is a …set of configurations or policies enforced by an EACMS… This definition doesn’t establish a boundary (logical border) so the language outside of the Responsible Entity’s Electronic Security Perimeters (ESP) or within an ESP doesn’t work. The introduction of the converting functionality is interesting. We suggest reviewing the definition of ESP/IRA/EAP. Alternate proposal User-initiated real-time access by a person outside of BES Cyber System, using a routable protocol: • to a BES Cyber System; • through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a BES Cyber System • To Management Interfaces of a Shared Cyber Infrastructure; or • To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP. Reference User-initiated real-time access by a person from outside of the Responsible Entity’s Electronic Security Perimeters (ESP). using a routable protocol: • to a Cyber System within an ESP; • through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter; • To Management Interfaces of a Shared Cyber Infrastructure; or • To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5	
Answer	No
Document Name	

Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	

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

Comment	
N&ST believes the first sentence, "User-initiated real- time acces s by a person from outside of the Responsible Entity's Electronic Security Perimeters (ESP) using a routable protocol" fails to account for Responsible Entities that only have ESPs at some of their in-scope facilities or, in some instances (e.g., a TO with only serial Med Impact BCS) have no ESPs at all. Suggested change: "User-initiated real- time access by a person from outside of the Responsible Entity's Electronic Security Perimeters (ESPs) u sing a routable protocol, or "User-initiated real- time access by a person from outside of a Responsible Entity asset that contains only serially-connected BCS using a routable protocol… (etc.)"	
Likes 0	
Dislikes 0	

Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	
Answer	No
Document Name	

Comment	
The IRS SRC recommends the SDT clarify the second bullet under the Interactive Remote Access (IRA) definition because it does not apply to any NERC CIP applicable system. Suggest changing the language from: "through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;" to: "to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;".	
Likes 0	
Dislikes 0	

Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	

Answer	Yes
Document Name	
Comment	
Chelan agrees with the proposed definition changes for IRA.	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy generally supports the SDT's direction, but suggests several changes to address various concerns: Duke recommends that the second bullet be updated to read more clearly: "through a Cyber Asset or Virtual Cyber Asset that converts the communication from a routable protocol to a non-routable protocol that is passed on to a Cyber System not within an ESP." This also consistently applies abbreviations after the first instance of the term is spelled out. Duke has concerns with the application of the IRA definition to the Management Interfaces of EACMS that enforce ESPs. This may result in reliability impacts when an EACMS Firewall management interface can only be accessed by an IS that is secured in a DMZ behind that firewall, and a failure of the firewall prevents access to the IS. We would suggest that the last bullet be removed from the definition. Proposed requirements in CIP-005 R1 Part 1.2 should provide adequate protection for these interfaces. Finally, Duke Energy recommends that the SDT either explicitly refer to the defined term "Real-time" or use alternative language to avoid auditor interpretations as seen in the difference between "adverse impact" used in the BCA definition and the defined term "Adverse Reliability Impact".	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	

AZPS agrees with the proposed change to the IRA definition.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Agree with the change to IRA definition.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

6. The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The IRC SRC requests the SDT clarify the second bullet under the Management Interface definition; i.e. “Provide lights-out management capabilities; or,” by replacing vendor terminology with language from the prior Management Module definition; i.e. “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.”

Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing?

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Request clarification of the second bullet – “Provide lights-out management capabilities; or.” Suggest using the old language instead of a vendor’s term. The old language was “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.”

Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing?

The definition seems to be too specific, i.e. direct reference to SCI, LOM, and ESP. Why not a more generic and simple definition like

A user interface, logical interface, or dedicated physical port that is used to control the processes of initializing, deploying, and configuring a cyber asset, excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Reference

A user interface, logical interface, or dedicated physical port that is used to:

• Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or

• Provide lights-out management capabilities; or

• Configure an Electronic Security Perimeter; excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
The revised definition does provide improvement over what was provided in the last draft, however, additional clarity to the intended meaning of Management Interface is still needed. This may be possible through additional enhancements to the definition or through additional explanation/defining what a Management Interface is through the Rationale. EEI offers the following revised definition: *"A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems."*

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	

Comment
ATC understands the intent of the SDT and the rationale for Management Interface; however, the concepts of Management Plane and Operational Plane were clearer. While ATC appreciates the attempt to consolidate these terms and views Draft 2 as an improvement over Draft 1, 'interface' may be an overly broad term. The words 'user interface' are doing some heavy lifting and while the application interface and physical interface are performing the same "user interface" function, they really are very different things. There may be room for entities to misinterpret the current definition to their own peril. • Is the overall purpose to protect from lateral movement, or to protect from unauthorized access to a management system? • Is identity the primary perimeter?   ○ Would it help if the SDT considered that concept when reassessing this definition and corresponding requirement language? • The communication channel from which management is performed must be segregated from the channel with which operational functions are performed.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	

Comment
ERCOT supports the IRC SRC comments and offers this additional comment: • Please clarify whether the Management Interface includes configuration of BCSs and PCAs within the ESP.

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 disagrees with the addition of “Configure an Electronic Security Perimeter” to the Management Interface definition. With the definition of ESP being “a set of configurations or policies”, a Management Interface is something that configures a configuration that controls communications of any type at all. See Q14 for an example of the issues caused by this construct. Southern suggests that requirements be written that apply to BES Cyber Systems and separate requirements that set clear expectations around the use and administration of electronic access controls (and by extension PACS) and begin the process of moving away from an EACMS as a ‘device’ focus.	
Likes 0	
Dislikes 0	
Response	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	

ACES feels the inclusion of “Configure an Electronic Security Perimeter” does not cover what is intended and leaves a gap. We feel EACMS is a more inclusive term in place of ESP. Use of EACMS instead of ESP would then include Intermediate Systems, which pose a risk if Management Interfaces are not protected. This would then be consistent with the IRA definition.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan

Answer	No
Document Name	

Comment

OPG concurs with NPCC's RSC comments

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We agree with the Management Interface definition, but disagree with the language in the definition. In our view, the definition should focus on in CIP scope management interfaces. “Provide lights-out management capabilities” should be removed since this criterion cannot make a management interface to fall within CIP scope. Also, we suggest changing “configure ESP” to “configure EAP” and “configure EACMS” to address the zero-trust mode (See our comments in Q4). Also, the Management Interface definition only covers the Management Interface of a management system such as vCenter that configures and manage SCI while the Hypervisor Management Interface that initializes, deploys and configures VCAs is missing from the definition. Furthermore, the Management Interface should include managing non-ESP model based on our comments in Q4.

Recommendation: We propose the following changes to Management Interface definition and rationale in Q1.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

The term lights-out management capabilities is unclear. Additionally, in our opinion it should be specified that individual BCA or PCAs only controlling access to themselves (such as host-based firewalls) and their user interfaces do not classify as EACMs and Management Interfaces.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
In support of IRC SRC/SWG. Request clarification of the second bullet – “Provide lights-out management capabilities; or.” Suggest using the old language instead of a vendor’s term. The old language was “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.” Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing?	
Likes 0	
Dislikes 0	
Response	

Michael Brytowski - Great River Energy - 3	
Answer	No
Document Name	
Comment	
GRE agrees with the comments submitted by the NSRF.	
Likes 0	
Dislikes 0	
Response	

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE requests that a term other than "lights out" be used in the definition to avoid diffuclty with interpretation related to marketing language related to such products. Please re-cast the definition related to "lights out" management interfaces with respect to the character of the functions supported by the interface and the potential for risk to Cyber Asset support for reliability functions.	
Likes 0	

Dislikes 0	

Response

Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	

Comment
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
We agree with the Management Interface definition, but disagree with the language in the definition. In our view, the definition should focus on in CIP scope management interfaces. “Provide lights-out management capabilities” should be removed since this criterion cannot make a management interface to fall within CIP scope. Also, we suggest changing “configure ESP” to “configure EAP” and “configure EACMS” to address the zero-trust mode (See our comments in Q4). Also, the Management Interface definition only covers the Management Interface of a management system such as vCenter that configures and manage SCI while the Hypervisor Management Interface that initializes, deploys and configures VCAs is missing from the definition. Furthermore, the Management Interface should include managing non-ESP model based on our comments in Q4.

Recommendation: We propose the following changes to Management Interface definition and rationale in Q1.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Request clarification of the second bullet – “Provide lights-out management capabilities; or.” Suggest using the old language instead of a vendor’s term. The old language was “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.” Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing? The definition seems to be too specific, i.e. direct reference to SCI, LOM, and ESP. Why not a more generic and simple definition like A user interface, logical interface, or dedicated physical port that is used to control the processes of initializing, deploying, and configuring a cyber asset, excluding physical user interfaces (e.g., power switch, touch panel, etc.). Reference A user interface, logical interface, or dedicated physical port that is used to: • Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or • Provide lights-out management capabilities; or • Configure an Electronic Security Perimeter; excluding physical user interfaces (e.g., power switch, touch panel, etc.).	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	

Comment
AEP supports EEI comments and revised definition on “Management Interface”. In addition, please see response to Question #14 related to nesting acronyms within definitions. The revised definition for SDT’s consideration reads: *“A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems.”*

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1	
Answer	No
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	

Comment
In support of NPCC RSC comments. Request clarification of the second bullet – “Provide lights-out management capabilities; or.” Suggest using the old language instead of a vendor’s term. The old language was “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.” Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing? The definition seems to be too specific, i.e. direct reference to SCI, LOM, and ESP. Why not a more generic and simple definition like

A user interface, logical interface, or dedicated physical port that is used to control the processes of initializing, deploying, and configuring a cyber asset, excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Reference

A user interface, logical interface, or dedicated physical port that is used to:

• Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or

• Provide lights-out management capabilities; or

• Configure an Electronic Security Perimeter; excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0	
Dislikes 0	

Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	

Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: Request clarification of the second bullet – “Provide lights-out management capabilities; or.” Suggest using the old language instead of a vendor’s term. The old language was “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.” Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing?	
Likes 0	
Dislikes 0	

Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI Comments

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Additional clarity is required around the concept of "user interfaces" that are in scope per the new definition vs. the physical user interfaces that are indicated as being out of scope. This is a confusing and contradictory element of the definition. The definition is very broad and would include interface ports such as PS2 mouse/keyboard ports. It is not clear as to how practical considerations of such ports that have connected mice and keyboards for example would need to be protected per the CIP-005-8 proposed standard requirements to permit only needed and controlled communications to and from Management Interfaces and deny all other communications. Alternatively, as an example, it is not clear from a practical sense of how, per CIP-007-7, one would prevent the sharing of the CPU and memory of keyboard/mouse user interface ports.

BC Hydro recommends changing the reference per the bullet "Provide lights-out management capabilities' within the definition of Management Interface to a more generic reference such as "out-of-band management capabilities" to meet the security intent instead of limiting to a particular type/brand.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment
SIGE does not agree with the new Management Interface definition, because it singles out a few Cyber Systems within the definition. The definition should define what a Management Interface is, and the standards/requirements will pinpoint which Cyber Systems should be applied. SIGE proposes the following: “A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems.”

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	

Comment
NCPA support the modified definition, but suggest the language out-of-band instead of lights-out, since it a more general industry term and associated with a particular vendor.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	

Comment
CEHE does not agree with the new Management Interface definition, because it singles out a few Cyber Systems within the definition. The definition should define what a Management Interface is, and the standards/requirements will pinpoint which Cyber Systems should be applied. CEHE proposes the following: “A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems.”

Likes 0	

Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Request clarification of the second bullet – “Provide lights-out management capabilities; or.”	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
ACES feels the inclusion of “Configure an Electronic Security Perimeter” does not cover what is intended and leaves a gap. We feel EACMS is a more inclusive term in place of ESP. Use of EACMS instead of ESP would then include Intermediate Systems, which pose a risk if Management Interfaces are not protected. This would then be consistent with the IRA definition. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	

We support the general approach. However, the language is written using “or”. As a result, a management interface that supports any lights out system. In cases such as CIP-007 R1.3, this may be inappropriately interpreted to bring in unrelated items such as a UPS that support these devices.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	No
Document Name	

Comment

AZPS agrees with the proposed definition included in EEIs comments filed in this matter. AZPS requests additional information on what “Lights-Out capabilities”includes.

Proposed Definition: “*A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems.”*

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

The proposed definition leaves a great deal of ambiguity about the intent of the ‘user interface, logical interface, or dedicated physical port’. While in most cases, an entity would likely choose to go to the physical or logical (VLAN/sub-interface) port level, there are concerns about an approach where the entity may try to only protect the user interface, leaving other ports (TCP/UDP) on the same physical/logical port unprotected. It is unclear how vCenter would be treated – MRO would interpret it to be a ‘user interface’ included with SCI (per SCI definition, “including the software and Management Interfaces”).

In an all-in scenario, how do the protections apply to a Management Interface that is a different Cyber Asset (CA) from the SCI. For example, if vCenter is a different CA than the SCI its managing, how does the applicability of in CIP-005, CIP-007 and CIP-010 extend to that different CA running vCenter become SCI identified independently or a Cyber Asset?

The SCI definition includes Management Interfaces, if the Management Interface is a separate Cyber Asset how does the applicability extend to the separate Cyber Asset? For example, if a central firewall management system is outside of the ESP, how would this system be protected in the all-in scenario, or will it be required to be inside an ESP?

Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
The proposed changes appear to require significant modification to our current network architecture without clearly indicating how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy supports a consolidated definition for the various management components that require protection but suggests the use of “Management System” instead of “Management Interface” for parity with BCS, Cyber System, etc. as the preferred terminology for Applicable Systems. Additionally, Duke requests that the SDT provide thorough implementation guidance to assist in correctly classifying systems that provide management functions but	

are not associated specifically with SCI (e.g. SCOM) as this definition may introduce a confusing break in consistency of classification between SCI management (e.g. vCenter) and other management tools.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The previously proposed term “Management Systems” provided better clarity for identification of systems that support patching, configuration management, anti-malware signature updates, and other management functions. This clarity was lost with the newly proposed term. Specifically, the ‘and’ clause in “Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure;’ seems to imply only inclusion of systems used for initial provisioning (e.g., installing an operating system & configuring a network card) as opposed to systems that supporting ongoing health and maintenance activities for deployed systems.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	

The inclusion of “user interface” within the Management Interface definition will overly broaden the impact of the proposed definition. NRG recommends removing “user interface” from the definition.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

The inclusion of “user interface” within the Management Interface definition will overly broaden the impact of the proposed definition. NRG recommends removing “user interface” from the definition.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

There appears to be ambiguity around what is meant by logical interface. Does “user interface” refer to graphical user interface? If not, what is the difference between a “user interface” and the excluded “physical user interfaces…”?

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	Yes
Document Name	

Comment

No comments

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	Yes
Document Name	

Comment

Defining the Management Interface is good however documenting in the CIP-002 when used as part of the SCI should be clarified.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	Yes
Document Name	

Comment

Agree with the modified Management Interface definition.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	Yes
Document Name	

Comment

No comment.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

The proposed changes are an improvement to the previous Management Module and Management Systems definition; however additional clarity could be provided when referring to "lights-out" management capabilites. All entities may not agree on the intent of the referenced term, it should be defined to address the ability for a system administrator to monitor and manage servers by remote control.

Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

iLO is a branded technology for Hewlett-Packard. BPA suggests replacing “lights-out” terminology with “dedicated out-of-band”.

Likes 0	

Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
With the improvements to scoping in Draft 2, Chelan agrees with the definition Management Interface.	
Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	

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

Comment	
Likes 0	
Dislikes 0	

Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	

Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
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	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends clarifying the definition of Management Interface. It is unclear what the three terms user interface", "dedicated physical port", and "physical user interfaces mean. Texas RE recommends the following definition:	

Management Interface: Any interface that is used to provide interactive electronic access and: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or • Provide lights-out management capabilities; or • Configure an Electronic Security Perimeter

Likes 0	
Dislikes 0	

Response

7. As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
NRG believes that the modified ESP definition reduces the burden of documenting ESPs in a zero trust environment. However, the modified ESP definition over complicates the documentation of ESPs in a traditional, firewall-based environment.	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG believes that the modified ESP definition reduces the burden of documenting ESPs in a zero trust environment. However, the modified ESP definition over complicates the documentation of ESPs in a traditional, firewall-based environment.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
There is insufficient clarity provided within the proposed terms to ensure that consistent understanding of the construct of policy – e.g.: whether policy refers to technical control or procedural document.	
Likes 0	

Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	

Comment
Xcel Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
BPA agrees that this will reduce the burden of documenting ESPs in a zero trust environment. However, additional language is needed to address whether the drafting committee still intends for standalone networks that have no external connectivity to other networks (”standalone networks”) to have a defined ESP. **Option 1**: If standalone networks DO NOT require an ESP, please update the Technical Rationale to address standalone networks (as was traditionally done in the **TR for CIP-005-6 and CIP-005-7**). **Option 2**: If standalone networks DO still require an ESP, the proposed definition requires all ESPs to be “enforced by an EACMS;” this will add a high burden for standalone networks. For example, a standalone ESP consisting of a local operator HMI (PCA, used for local review of SCADA alarms) connected to 2 local SCADA RTUs (BCAs) via a switch (PCA) would need to have an EACMS added in order to meet the letter of the requirement, but without gaining any security or protection. (1) Definition for Electronic Security Perimeter (ESP): A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs. Benefit: This would permit the isolated nature – or “configuration” – of the small local network to provide the control of communications to/from the BES Cyber System by simply excluding it. (2) Add an additional requirement under CIP-005-8 R1.1 [hypothetically referenced here as R “1.1-A” for numbering clarity] for the EACMS portion: Requirement: 1.1-A Applicable Systems: BCS with ERC and their associated PCA

Requirements: Utilize an EACMS to enforce the control of communications to or from any part of a BES Cyber System.

(3) Related update is needed to correct the Applicable Systems in R2.1: “EACMS that enforces an ESP for the Applicable Systems in Part 1.1-A.”

(4) Update the Technical Rationale (TR) to clarify for standalone networks (as was traditionally done in the TR for CIP-005-6 and CIP-005-7).

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Although Duke Energy disagrees with the inclusion of “policy” in the definition, the spirit of this modified definition provides explicit clarity that evolving security technologies can be used in compliance with the NERC CIP Standards and will assist Registered Entities and the ERO in documenting CIP-005 compliance with increasingly secure postures.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	No
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Josh Johnson - Lincoln Electric System - 1

Answer	No
Document Name	

Comment
We disagree based on the reasoning and alternative proposal outlined in question 4.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	

Comment
AZPS doesn't understand how the use of "configurations or policy" in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	

Comment
While Zero Trust and it's assumption of assuming no network edge is an excellent security approach, it is necessary to ensure that a discrete boundary defines the edge of the auditable network. The current definitions significantly blur this border introducing uncertainty into what will be audited under the CIP standards and introduces opportunity for significantly different viewpoints between auditors and entities regarding the boundary of what will be subject to NERC compliance standards. We support adopting definitions and standards that support virtualization. However until this is resolved, it will be impossible to support the revised standards. We recommending basing the new definition around the previous definition of an ESP as it has a defined border.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No

Document Name	
Comment	

ACES feels no matter how zero trust environments are implemented, the policy (ies) or configurations will be highly complex and exponentially more difficult to prove strict compliance, thus increasing compliance burden. Additionally on the latest webinar, it was discussed each policy enforcement point would be an EACMS. In a Cisco based SDN, each switch port, switch port group, VLAN, or switch has an enforcement policy applied to it from the policy server, increasing the number of EACMS significantly, therefore increasing compliance burden.

Another issue will be varying technology compared to firewall rules/ACL as used today. This will make auditing extremely complex and require an auditor to have significant knowledge of varying SDN/zero trust products to be able to accurately audit.

AEPC has signed on to ACES comments.

Likes 0	
Dislikes 0	
Response	

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	
Comment	

We are not sure it reduces the burden as entities will have to prove to auditors they are compliant and we don't know at this point what audit evidence requests will look like. We also wish to verify that knowledge of the TR is not necessary for understanding or complying with the proposed revisions to CIP-005-X R1.

Likes 0	
Dislikes 0	
Response	

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	
Comment	

NCPA supports most of the definition change, however "policies" are a vague reference. NCPA proposes using the phrase "technical policies" as to not confuse them with administrative policies.

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
While it may be the SDT's intent to reduce ESP documentation burden for entities employing Zero Trust environments, the language of the standards themselves do not reduce any such documentation burden pertaining to ESPs. In fact, the requirements still require ESPs to be implemented. BC Hydro recommends adding clarifying language around documentation expectations when Zero Trust environments are implemented vs. traditional firewall bounded ESPs.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	

MEAG Power adopts the Southern Company comments.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

We support NPCC TFIST's comments as found below:

We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment.

Looking solely at the definition of ESP, the old definition required to simply produce a list of assets in a boundary, this resulted in a large ESP. Establishing these ESP was easy and there were only one criteria to evaluate (connected using a routable protocol), overall (less burden). The suggested definition permits potentially smaller ESP, so more ESP, but those ESPs come with more controls, i.e., configurations or policies enforced and EACMS. With the new definition, the burden of the demonstration is more.

The ideas behind the new definition are interesting and they could facilitate the instauration of a zero-trust environment, but those ideas don’t lessen the burden of compliance demonstrations.

Reference:

Old Definition: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

Suggested Definition: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP agrees with EEI's concern that it is unclear how the use of the terms "configuration or policy" reduces the burden of documenting ESPs in a zero trust environment. AEP also supports EEI's recombination on providing additional clarity and examples. In addition, AEP suggests the removal of the second sentence in the proposed ESP definition as noted in response to Question #4 above.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment.

Looking solely at the definition of ESP, the old definition required to simply produce a list of assets in a boundary, this resulted in a large ESP. Establishing these ESP was easy and there were only one criteria to evaluate (connected using a routable protocol), overall (less burden). The suggested definition permits potentially smaller ESP, so more ESP, but those ESPs come with more controls, i.e., configurations or policies enforced and EACMS. With the new definition, the burden of the demonstration is more.

The ideas behind the new definition are interesting and they could facilitate the instauration of a zero-trust environment, but those ideas don't lessen the burden of compliance demonstrations.

Reference:

Old Definition: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

Suggested Definition: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 3	
Answer	No
Document Name	
Comment	
GRE has not seen how the modified ESP definition can reduce the burden of documenting ESPs in a zero-trust environment (see NSRF comments in Q4). Given that a zero-trust environment in virtualization layer is a non-ESP topology and ESP drawings are not needed, there is no compliance burden reduction. Resulting from our comments in Q4, the zero-trust model can be resolved by adding an alternative requirement in CIP-005 R1.1.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
In support of IRC SRC/SWG. We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

Regardless of which direction we go in will always have a burden - and again each entity will still have to show the auditors we are compliant. Depending on the auditor and their intreption of the requirement - can become burdensome. We don't understand the zero trust environment as defined.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

We are concerned that in hybrid environments with traditional firewalls AND zero-trust or host-based firewall applications, the new definitions of ESP and EACMs could create a burden to industry by requiring additional protections (such as encryption and multifactor authentication) on communications between devices that are already protected inside an ESP by a traditional firewall, and actually discourages the use of multi-layered protection.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We haven't seen the modified ESP definition can reduce the burden of documenting ESPs in a zero-trust environment (see our comments in Q4). Given that a zero-trust environment in virtualization layer is a non-ESP topology and ESP drawings are not needed, there is no compliance burden reduction. Resulting from our comments in Q4, the zero-trust model can be resolved by adding an alternative requirement in CIP-005 R1.1.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment
• The ESP definition enables virtualization and logical boundaries but is not really going to reduce the documentation load. Zero trust will require documentation of where controls are applied including locations. • The IP to serial conversion for ERC and IRA appears to require additional documentation beyond the ESP. Please clarify how Entities are expected to document the logical boundaries beyond the ESP for serial devices.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5	
Answer	No
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	

Comment
OPG concurs with NPCC's RSC comments

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6	
Answer	No
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	

Comment
Eversource agrees with the modified ESP definition, however, Eversource does not agree this change reduces the documentation burden of ESPs in a zero-trust environment.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	

Comment
ACES feels no matter how zero trust environments are implemented, the policy (ies) or configurations will be highly complex and exponentially more difficult to prove strict compliance, thus increasing compliance burden. Additionally on the latest webinar, it was discussed each policy enforcement point would be an EACMS. In a Cisco based SDN, each switch port, switch port group, VLAN, or switch has an enforcement policy applied to it from the policy server, increasing the number of EACMS significantly, therefore increasing compliance burden. Another issue will be varying technology compared to firewall rules/ACL as used today. This will make auditing extremely complex and require an auditor to have significant knowledge of varying SDN/zero trust products to be able to accurately audit.

Likes 0	
Dislikes 0	

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer	No
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	
AWS supports the implementation of zero-trust architectures in fulfilling the security objectives of the NERC CIP Standards, but is seeking clarity on the assertion that the use of configurations or policies in the modified ESP definition can reduce the burden of documenting ESPs in a zero-trust environment. In a zero-trust environment the ESPs implemented by a Responsible Entity become more granular increasing the compliance documentation needed to support each policy or set of policies applied.	
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 agrees with the focus on network access policies rather than strictly network subnets (while not disallowing it) as things progress towards zero trust. However, as more fully stated in Q4, the phrase “that control communications” is overly broad and the ESP definition has nothing that scopes it to network communications.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT supports the IRC SRC comments.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
It is unclear how the use of the terms “configuration or policy” reduces the overall burden of documenting ESPs in a zero-trust environment. Zero trust is not used under the current definition of ESPs within a substation environment and for those entities that plan to continue using traditional firewalls, their processes for maintaining documentation will remain unchanged. For this reason, EEI requests additional clarity and examples describing how the use of “configuration or policy” language in this definition reduces the current burdens of documenting ESPs.	
Likes 0	
Dislikes 0	
Response	

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment. Looking solely at the definition of ESP, the old definition required to simply produce a list of assets in a boundary, this resulted in a large ESP. Establishing these ESP was easy and there were only one criteria to evaluate (connected using a routable protocol), overall (less burden). The suggested definition permits potentially smaller ESP, so more ESP, but those ESPs come with more controls, i.e., configurations or policies enforced and EACMS. With the new definition, the burden of the demonstration is more. The ideas behind the new definition are interesting and they could facilitate the instauration of a zero-trust environment, but those ideas don't lessen the burden of compliance demonstrations. Reference: Old Definition: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol. Suggested Definition: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	
Answer	No
Document Name	
Comment	
The IRC SRC agrees with the modified ESP definition; however, we disagree this change will reduce the burden of documenting ESPs in a zero-trust environment.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	

Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Chelan agrees with the change to ESP, but disagrees with the notion that the new definition reduces the burden of documenting ESPs in a zero trust environment, rather it simply enables zero trust to even be an option.	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
We agree with the modified ESP definition but are not sure it reduces the burden as entities will have to prove to auditors they are compliant and we don't know at this point what audit evidence requests will look like. We would also like to point out that because the routable protocol qualifier was eliminated from the ESP definition, and changes to the CIP-005 R1 Part 1.1, serial connectivity in some cases has been brought into the scope of an ESP. Refer to question #10 below.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	

Answer	Yes
Document Name	
Comment	
Suggest removing ‘and their associated PCAs’ from the ESP definition as PCAs are already included in the CIP Systems definition. ‘These configurations or policies group CIP Systems of the same impact rating (and their associated PCAs) delete this.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE proposed an ESP definition in response to question #4. However, it maintained the SDT approach on the use of configurations or policy. This does seem to have the potential of reducing the burden of documenting ESPs in a zero-trust environment.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE proposed an ESP definition in response to question #4. However, it maintained the SDT approach on the use of configurations or policy. This does seem to have the potential of reducing the burden of documenting ESPs in a zero-trust environment.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	

Answer	Yes
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Yes, although PNMR appreciates EEI suggestion regarding "...clarity and examples describing how the use of “configuration or policy” language in this definition reduces the current burdens of documenting ESPs."	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment
We agree with the modified ESP definition but are not sure it reduces the burden as entities will have to prove to auditors they are compliant and we don't know at this point what audit evidence requests will look like. We would also like to point out that because the routable protocol qualifier was eliminated from the ESP definition, and changes to the CIP-005 R1 Part 1.1, serial connectivity in some cases has been brought into the scope of an ESP.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends registered entities continue documenting ESPs in order to demonstrate compliance and show evidence of configuration of a zero-trust environment.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power has no experience with zero trust environments and has no feedback.	
Likes 0	
Dislikes 0	
Response	

8. The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Dan Zollner - Portland General Electric Co. - 3

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Portland General Electric Company has concerns regarding the Interactive Remote Access (IRA) defintion. In the second bullet of the definition, the clause "to a Cyber System not within an Electronic Security Perimeter" implies that IRA can exist in scenarios where a person has no intent of remotely connecting to a BES Cyber System or PCA. The proposed definition of a Cyber System includes any number of Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that may be either CIP or non-CIP. If an individual was remotely communicating through a protocol converter to a device like a PACS, EACMS, or non-CIP Cyber Asset existing outside the ESP, that would be considered IRA under the current definition even if those systems didn't have connectivity to a BES Cyber System. Portland General Electric Company believes changing the clause to "to a BES Cyber System not within an Electronic Security Perimeter" achieves the objective of controlling IRA to BES Cyber Assets that are serially connected to the BES Cyber System.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The IRC SRC requests the SDT clarify ERC for serial – IP communications to ensure backwards compatibility. We understand the proposed definition will not be backwards compatible; e.g. CIP-005, R3.1 and CIP-007, R4.2. Is that correct?

In addition, we request the SDT clarify the definition for BES Cyber System Information (BCSI) to include “SCI identified independently, supporting an Applicable System.”

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

N&ST recommendations for the definitions of ERC, ESP, and IRA are in our responses to Questions 3, 4 and 5, respectively. N&ST respectfully suggests the following changes to these additional definitions:

> EAP: “A policy enforcement point or a Cyber Asset interface that controls routable communication to and from a BES Cyber System from outside its Electronic Security Perimeter.”

> IS: The statement within the current IS definition, “The Intermediate System must not be located inside the Electronic Security Perimeter,” should be retained.

> EACMS and PACS: N&ST recommends both definitions, which begin with “Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI),…” be modified to begin with, “Cyber Assets, Virtual Cyber Assets, Cyber Systems, or Shared Cyber Infrastructure (SCI),…” This would clarify that it’s permissible to group an SCI with the EACMS and/or the PACS it supports.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Portland General Electric Company has concerns regarding the Interactive Remote Access (IRA) defintion. In the second bullet of the definition, the clause "to a Cyber System not within an

Electronic Security Perimeter" implies that IRA can exist in scenarios where a person has no intent of remotely connecting to a BES Cyber System or PCA. The proposed definition of a Cyber System includes any number of Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that may be either CIP or non-CIP. If an individual was remotely communicating through a protocol converter to a device like a PACS, EACMS, or non-CIP Cyber Asset existing outside the ESP, that would be considered IRA under the current definition even if those systems didn't have connectivity to a BES Cyber System. Portland General Electric Company believes changing the clause to "to a BES Cyber System not within an Electronic Security Perimeter" achieves the objective of controlling IRA to BES Cyber Assets that are serially connected to the BES Cyber System.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2

Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.”

We suggest some additional work on the definitions (ESP/IRA/CIP System/SCI) and a better alignment with the current CIP language.

Also, some definition includes some requirements on CPU and memory (isolation/shared), those requirements are not future proof. Furthermore, the definitions by focusing on shared CPU and memory trend toward hypervisor-based virtualization and don’t seem to provide a clear framework around other types of virtualizations like containerization technology.

We Suggest that the SDT review the definitions, the need for defining new terms and the nested definitions.

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

see responses to previous questions

Some additional revisions:

Remove “TCA” from CIP Systems - A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, or Shared Cyber Infrastructure, or Protected Cyber Asset. [delete - or Transient Cyber Asset.]

Remove “or a PCA” from the Virtual Cyber Asset - A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure [delete - or a PCA.]

Add “protocol” to EAP - A policy enforcement point or a Cyber Asset interface that allows routable protocol communication to and from the BES Cyber System within an Electronic Security Perimeter.

Cyber Asset – consider not excluding SCI, keeping the original - Programmable electronic devices, including the hardware, software, and data in those devices; [delete - excluding Shared Cyber Infrastructure.]

Cyber System – we suggest reverting back to Cyber Assets where this is used or go with a generic “cyber system” term in the exemptions language. Leave cyber system an undefined term. Simplifying applicability can create increased scope in the requirements.

Shared Cyber Infrastructure – Please provide more information in the technical rationale on what is intended with “including the software.”

Management Interface – In the non-virtualized environments there are applications that manage the policy implementation of firewalls that would be both a Management Interface and an EACMS under the new requirements and definitions. Was this the SDT’s intent?

Likes 0	
Dislikes 0	

Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	

PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

Regarding ERC, this is a substantial change to the definition of ERC that has a larger impact than in the context of addressing virtualized environments.

Several of the terms have been removed from the proposed definitions but are still being used other definitions and standards. For example Management Systems and Management Module have been removed but are still used in the SCI definition and in the CIP-005 R2.1 Measures and through the CIP-005 violation severity levels.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Generally, EEI supports most of the new/revised terms, but we have concerns with the following terms:

External Routable Connectivity (ERC): See our comments to Question 3 above.

Electronic Security Perimeter (ESP): See our comments to Questions 4 and 7 above.

Interactive Remote Access (IRA): See our comments to Question 5 above.

Management Interface: EEI disagrees with the practice of nesting other Glossary Terms within the definition of other Glossary Terms. This practice makes it difficult to support definition that might otherwise be supported. While there are a number of other examples of this practice (see SCI) Management Interface serves as a good example of our concern.

Protected Cyber Asset (PCA): EEI seeks additional clarifications on the qualifier of "excluding Virtual Cyber Assets that are being actively remediated prior to introduction to the ESP." If the VCA, or physical Cyber Asset, is outside of the ESP, how could it be considered a PCA when the required attribute of a PCA is that it is inside an ESP? Please provide clarification.

Virtual Cyber Asset (VCA) – The current definition is unclear and possibly unnecessary given the intent is to simply provide an equivalent virtualized term for a Cyber Asset, which is not a system but a programmable electronic device. If the SDT believes this term is necessary, we suggest the following:

"A logical instance of a programmable device, including the software and data, hosted on Shared Cyber Infrastructure or a PCA."

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC continues to have some questions about ERC and devices wholly inside an ESP.

- Where does the chain end?
- Do Cyber Assets two hops removed from the IRA entry point inside the ESP, or the system to system routable communication path between a system inside and outside the ESP have ERC?

The use of the term asset may make it more difficult to determine where ERC exists. Non-CIP systems inside a Control Center "asset" that are connecting into a CIP System inside the same Control Center "asset" could be at varied trust levels and should be protected via ERC and IRA controls.

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	

Comment

ERCOT supports the IRC SRC comments and offers this additional comment:

- SCI should not be excluded from the Cyber Asset definition. SCI meet the definition of Cyber Asset in that it is comprised of hardware, software, and data.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

LCRA is concerned with using CIP System incorrectly due to SDT intent to only use it as a “non-CIP System”. CIP System does not appear to be a necessary term. TCAs are included in the CIP System definition. However, CIP System is used in the definition of ESP. This is an example of the confusion associated with the term.

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

For “CIP System”, Southern agrees with having defined terms as shorthand, such as in CIP-007 R1.3 with its use of “non-CIP Systems.” However, Southern disagrees with the inclusion and nesting of this broad term within *many other* definitions. Analyzing the resulting scope of nested definitions based on “CIP System” is problematic, and our answers to Q3 and Q4 are specific examples of issues in its inclusion in ERC and ESP definitions.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	

In addition to the comments regarding the ESP definition provided in response to question 4, AWS offers comments on the terms: CIP System, Cyber System and Transient Cyber Asset.

The terms CIP System and Cyber System are similar and could easily be confused or misunderstood. Please clarify whether the term “System” implies that evidence of compliance can be presented at the system level rather than the device level.

In addition, we oppose and suggest reconsideration to the Transient Cyber Asset (TCA) definition revision that allows virtual machines running on a physical TCA to be treated as software on the device. As written, a Responsible Entity is not be required to apply the appropriate security controls to the virtual machines running on physical TCAs. For security purposes, Responsible Entities should be monitoring the state of the virtual machines running on their physical hardware for security issues. We propose removing the language “Virtual machines hosted on a physical TCA can be treated as software on that physical TCA” from the TCA definition, and modifying the VCA definition to read, “A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure, a PCA, or a TCA.”

Likes 0	
Dislikes 0	
Response	

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	

<duplicate>

Likes 0	
Dislikes 0	
Response	

James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	

LCRA is concerned with using CIP System incorrectly due to SDT intent to only use it as a “non-CIP System”. CIP System does not appear to be a necessary term. TCAs are included in the CIP System definition. However, CIP System is used in the definition of ESP. This is an example of the confusion associated with the term.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- The ERC and IRA with serial conversion needs to be clarified with more industry use cases and may require improved language.
- External Routable Connectivity (ERC) language enhancement: The electronic bidirectional routable protocol communications between a CIP System and a Cyber System (Cyber Asset or Virtual Cyber Asset) located outside of the asset's PSP or ESP.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

We believe the definition of ERC is confusing because it is unclear what the term "asset" is referring to when it states "from outside the asset containing the CIP System". Is this referring to a cyber asset, a BES asset, or a Facility? The definition was much clearer when referring to an ESP. The additional concerns with definitions have been addressed above.

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	No
Document Name	

Comment
Remove “TCA” from CIP Systems - A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, or Shared Cyber Infrastructure, or Protected Cyber Asset. [delete - or Transient Cyber Asset.] Remove “or a PCA” from the Virtual Cyber Asset - A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure [delete - or a PCA.] Add “protocol” to EAP - A policy enforcement point or a Cyber Asset interface that allows routable protocol communication to and from the BES Cyber System within an Electronic Security Perimeter. Cyber Asset – consider not excluding SCI, keeping the original - Programmable electronic devices, including the hardware, software, and data in those devices; [delete - excluding Shared Cyber Infrastructure.] Cyber System – we suggest reverting back to Cyber Assets where this is used or go with a generic “cyber system” term in the exemption's language. Leave cyber system an undefined term. Simplifying applicability can create increased scope in the requirements. Shared Cyber Infrastructure – Please provide more information in the technical rationale on what is intended with “including the software.”

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	

Comment
In support of IRC SRC/SWG. Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2 Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.”

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	

Comment
ISO-NE requests that a term other than "lights out" be used in the Management Interface definition to avoid diffuclty with interpretation related to marketing language related to such products. Please re-cast the definition related to "lights out" management interfaces with respect to the character of the functions supported by the interface and the potential for risk to Cyber Asset support for reliability functions.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	

Comment
See responses to previos questions. Remove “TCA” from CIP Systems - A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, or Shared Cyber Infrastructure, or Protected Cyber Asset. **or Transient Cyber Asset**. Remove “or a PCA” from the Virtual Cyber Asset - A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure **or a PCA**. Add “protocol” to EAP - A policy enforcement point or a Cyber Asset interface that allows routable protocol communication to and from the BES Cyber System within an Electronic Security Perimeter. Cyber Asset – consider not excluding SCI, keeping the original - Programmable electronic devices, including the hardware, software, and data in those devices; **excluding Shared Cyber Infrastructure**. Cyber System – we suggest reverting back to Cyber Assets where this is used or go with a generic “cyber system” term in the exemptions language. Leave cyber system an undefined term. Simplifying applicability can create increased scope in the requirements. Shared Cyber Infrastructure – Please provide more information in the technical rationale on what is intended with “including the software.” Management Interface – In the non-virtualized environments there are applications that manage the policy implementation of firewalls that would be both a Management Interface and an EACMS under the new requirements and definitions. Was this the SDT’s intent?

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No

Document Name	
Comment	
See comments in Q#5 above. With regard to EEI's comment regarding definition of VCA PNMR disagrees that it needs to be altered to better conform with the Cyber Asset definition. SMEs within our company found the definition proposed by the SDT to be clearer and a better fit than the definition proposed by EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No

Document Name	

Comment

Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2

Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.”

We suggest some additional work on the definitions (ESP/IRA/CIP System/SCI) and a better alignment with the current CIP language.

Also, some definition includes some requirements on CPU and memory (isolation/shared), those requirements are not future proof. Furthermore, the definitions by focusing on shared CPU and memory trend toward hypervisor-based virtualization and don’t seem to provide a clear framework around other types of virtualizations like containerization technology.

We Suggest that the SDT review the definitions, the need for defining new terms and the nested definitions.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Minnesota Power has concerns about acronyms CSI and SCI being confused. The SDT needs to consider other terms as it is close to an existing one. The SDT should consider *Private Cloud Infrastructure (PCI)* or *Virtual Cloud Infrastructure (VCI)* which could help facilitate a move to Public Cloud Infrastructure should an entity decide to do so. The second term may provide more flexibility in utlizing public cloud resources where an entity decides public cloud is more effective.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment
In general, AEP supports most of the new and revised terms, but we have concerns with the following terms: • **BES Cyber System Information (BCSI)**: There is no need to call out SCI in the BCSI definition when it is already covered in BES Cyber System definition. • **Cyber Assets**: While the exclusion of Shared Cyber Infrastructure (SCI) in Cyber Assets definition seems okay upfront, it gets very confusing when applying this definition along with other definitions, such as SCI and Virtual Cyber Asset (VCA). VCA definition says it might be hosted on SCI (i.e., "A logical instance of an operating system or firmware hosted on SCI or a PCA"); However, SCI definition says "SCI does not include the supported VCA or CA with which it shares its resources". Implementation may become chaotic unless all four definitions of CA, VCA, SCI and PCA are all logically explained in a real life context. • **External Routable Connectivity (ERC)**: See response to Question #3 above • **Electronic Security Perimeter (ESP)**: See responses to Questions #4 and #7 above. • **Interactive Remote Access (IRA)**: See response to Question #5 above. • **Management Interface**: See response to Question #6 above. • **Protected Cyber Asset (PCA)**: AEP seeks additional clarifications on the qualifier of "excluding VCA that are being actively remediated prior to introduction to the ESP." If the VCA, or physical Cyber Asset, is outside of the ESP, how could it be considered a PCA when the required attribute of a PCA be that it is inside an ESP? Please provide clarification. • **Shared Cyber Infrastructure (SCI)**: AEP in general supports the definition of SCI except for "identified independently" and the nested inclusion of the Management Interface term. Please see responses to Questions #2 and #6. • **Transient Cyber Asset (TCA):** AEP seeks additional clarifications on the significance of "Virtual machines hosted on a physical TCA can be treated as software on that physical TCA". If there were stated outcome(s) of treating as software, it might be more clear (implications of treating as software, that is).

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1	
Answer	No
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	

Comment
In support of NPCC RSC comments. Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2 Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.” We suggest some additional work on the definitions (ESP/IRA/CIP System/SCI) and a better alignment with the current CIP language. Also, some definition includes some requirements on CPU and memory (isolation/shared), those requirements are not future proof. Furthermore, the definitions by focusing on shared CPU and memory trend toward hypervisor-based virtualization and don’t seem to provide a clear framework around other types of virtualizations like containerization technology. We Suggest that the SDT review the definitions, the need for defining new terms and the nested definitions.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	

Comment
Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

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

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

Some additional revisions:

Remove “TCA” from CIP Systems - A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, or Shared Cyber Infrastructure, or Protected Cyber Asset. **(Remove: or Transient Cyber Asset.)**

Remove “or a PCA” from the Virtual Cyber Asset - A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure **(Remove: or a PCA)**.

Add “protocol” to EAP - A policy enforcement point or a Cyber Asset interface that allows routable protocol communication to and from the BES Cyber System within an Electronic Security Perimeter.

Cyber Asset – consider not excluding SCI, keeping the original - Programmable electronic devices, including the hardware, software, and data in those devices **(Remove: ; excluding Shared Cyber Infrastructure).**

Cyber System – we suggest reverting back to Cyber Assets where this is used or go with a generic “cyber system” term in the exemptions language. Leave cyber system an undefined term. Simplifying applicability can create increased scope in the requirements.

Shared Cyber Infrastructure – Please provide more information in the technical rationale on what is intended with “including the software.”

Management Interface – In the non-virtualized environments there are applications that manage the policy implementation of firewalls that would be both a Management Interface and an EACMS under the new requirements and definitions. Was this the SDT’s intent?

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

As stated in Question 3, we do not agree with the modification to the definition for ERC.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

We support NPCC TFIST's comments as found below:

Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2

Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.”

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	No
Document Name	

Comment

MEAG Power adopts the Southern Company comments.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI Comments

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
While the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the definitions associated with some of the proposed NERC Glossary terms per comments provided in this project comment/ballot submission.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	
The CIP standards as currently written are sufficient to accommodate virtualization based on security objectives. The proposed changes to the standards are overly prescriptive and difficult to understand. The previous proposed revision of the standards by this Project also adequately expanded the potential use of virtualization without removing backwards compatibility. Such drastic changes will be difficult to comply with and pose a security risk to the grid as time is taken away from practicing security and applied towards implementing overyly prescriptive compliance requirements that seem to be a hall of mirrors.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE has listed below terms not previously covered by the questions above. **CIP System** – Agree **Cyber Assets –** Agree	

Cyber System – Agree

EACMS – Agree.

EAP – Agree.

Intermediate Systems - Agree.

PACS – Agree

PCA – Agree

SCI – Agree

TCA – Agree

VCA – Since a VCA is a logical instance of a Cyber Asset it seems that the VCA definition should be like the Cyber Asset definition. The current proposed VCA definition is radically different than the Cyber Asset definition. For that reason, SIGE proposes:

"A logical instance of a programmable device, including the software and data, hosted on Shared Cyber Infrastructure or a PCA."

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA supports the proposed changes to IRA and Management Interface, however all others we do not support, please see comments above.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE has listed below terms not previously covered by the questions above.

CIP System – Agree

Cyber Assets – Agree

Cyber System – Agree

EACMS – Agree.

EAP – Agree.

Intermediate Systems - Agree.

PACS – Agree

PCA – Agree

SCI – Agree

TCA – Agree

VCA – Since a VCA is a logical instance of a Cyber Asset it seems that the VCA definition should be like the Cyber Asset definition. The current proposed VCA definition is radically different than the Cyber Asset definition. For that reason, CEHE proposes:

"A logical instance of a programmable device, including the software and data, hosted on Shared Cyber Infrastructure or a PCA."

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Several of the terms and their usage, especially SCI, lends ambiguity with their use in the Standards. Further clarifications and refinements of the terms should be given attention.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	
Comment	

Individually each new or revised term is acceptable. On the whole, however, it makes for a somewhat confusing “alphabet soup” of acronyms which only those with past experience in these technologies are easily able to tell apart or know which term is the appropriate one to use for which compliance tasks. The multiple new terms confuse efforts to comply and thus entail, even if only minor, more compliance risk rather than less. Further, it is not clear why all these terms are needed if we have an acceptable definition for Virtual Cyber Asset and a revised definition of BES Cyber System that includes Virtual Cyber Assets. We recommend the SDT review the definitions again to determine if few terms are needed and, if a new term is needed, to provide further clarity on what it addresses that other definitions do not.

Likes 0	
Dislikes 0	
Response	

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	
Comment	

Need to define/clarify “asset” in the definition of ERC,

Need clarification for the IRA definition (second bullet point is not clear)

Need clarification for “identified independently” in the definition of SCI

“CIP System” Definition – Transient Cyber Asset (TCA) should not be seen as a part of any system. A TCA is an asset connected to a system for a limited period of time. If it has to be seen as a part of a system, it is no longer a TCA. Also, this term is, in some ways, redundant compared to BCS. Even if “CIP System” designates any group of assets under CIP requirements, TCA cannot be seen as a “system”. It is an asset.

“Cyber System” Definition – Very confusing regarding “CIP System” and “BCS” definitions. Need more precisions or details about the context and when those definitions are used.

Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	
Comment	

We support adopting definitions and standards that support virtualization. However, it will be impossible to support the revised standards without a clearly defined demarcation of the auditable network infrastructure. We do not have a reasonable recommendation to meet this need using the current approach to the proposed CIP standards. The important items to consider are ensuring defined borders that clearly identify what is in and out of scope of the definitions, ensuring that a company that is implementing currently acceptable virtualization approach with high watermarking does not have extensive changes to their CIP programs, no inadvertent changes to compliance standards, and ensuring definitions that clearly separate hosts and guests within virtualization.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	No
Document Name	

Comment

AZPS does not agree with all changes to the NERC Glossary terms. AZPS agrees with the concerns included in EEIs comments filed in this matter regarding Cyber Assets and Virtual Cyber Assets.

Cyber Assets – This term should revert back to its original singular form. While the definition refers to programmable electronic devices, the term remains singular in form and intent. This change would also harmonize with the new definition for Virtual Cyber Asset, which is not pluralized.

Virtual Cyber Asset (VCA) – The current definition is unclear and possibly unnecessary given the intent is to simply provide an equivalent virtualized term for a Cyber Asset, which is not a system but a programmable electronic device. If the SDT believes this term is necessary, we suggest the following:

"A logical instance of a programmable device, including the software and data, hosted on Shared Cyber Infrastructure or a PCA."

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

CIP System – The definition contains an implicit requirement for entities to identify CIP Cyber Systems. The definition should not leave it up to the entity to make this identification, it should be criteria-based to include all of the described types of CAs. Alternate proposal: *A BES Cyber System and*

all associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, Shared Cyber Infrastructure, Protected Assets, and Transient Cyber Assets.

Transient Cyber Asset – The use of 'network within an Electronic Security Perimeter' no longer works with the new definition of ESP. Alternate proposal: replace 'network within an Electronic Security Perimeter' with 'network protected by an Electronic Security Perimeter'. (Even though the ESP definition no longer includes 'network', it is reasonable that a network could be protected by an ESP protecting all BCAs on that network.)

Removeable Media - The use of 'network within an Electronic Security Perimeter' no longer works with the new definition of ESP. Alternate proposal: replace 'network within an Electronic Security Perimeter' with 'network protected by an Electronic Security Perimeter'. (Even though the ESP definition no longer includes 'network', it is reasonable that a network could be protected by an ESP protecting all BCAs on that network.)

Likes 0	
Dislikes 0	

Response

Josh Johnson - Lincoln Electric System - 1

Answer	No
Document Name	

Comment

We disagree based on the reasoning and alternative proposal outlined in question 4.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	No
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Duke has a number of definition concerns that are enumerated in response to the specific questions where the definition is relevant. In addition to those concerns, Duke Energy believes the following definition changes are required for the successful implementation of 2016-02's goals:

CIP System – Duke Energy suggests removal of TCAs from this collection of other device types to ensure that there are no inadvertent changes to scoping that historically excluded TCA devices (e.g. list of Cyber Assets to be included on the ERT CA tab).

PACS/EACMS – definitions do not take advantage of the new Cyber System definition

Cyber System – Duke Energy suggests that the inclusion of the term group here may provide an auditor basis to expect REs to actively group things that otherwise would be passively addressed. Additionally, it would be helpful to clarify that Cyber Systems are not necessarily in CIP scope. Suggested language is as follows: One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure. Cyber Systems may or may not receive one or more NERC CIP classifications.

ESP – Duke notes that the proposed definition for ESP drops the term "boundary" which was helpful in ensuring that auditors correctly evaluated this term. We propose to add this concept back in a manner that supports future interpretation of how a boundary may be implemented. This helps to ensure that dependent definitions (e.g. PCA use of "within") remain compatible with this iteration of the standards. Duke's proposed definition is repeated from Question 4 here: "A set of configurations enforced by an EACMS that creates a logical boundary where communications to or from any part of a BES Cyber System and any PCA or SCIG associated with a BES Cyber System are controlled. All BCS, PCA, and SCIG included in an ESP have the same impact rating as the highest included device. The EACMS enforcing the ESP may not be part of a BES Cyber System."

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No

Document Name	
Comment	
The SDT should consider NIST based approaches focused on defined outcomes instead of being prescriptive based on existing technologies.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
As articulated in greater detail above in response to previous questions, NRG disagrees with several of the proposed changes to the NERC Glossary terms	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
As articulated in greater detail above in response to previous questions, NRG disagrees with several of the proposed changes to the NERC Glossary terms.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	No
Document Name	

Comment
The definition of PCA is problematic. The first is the general issue with the CPU/memory affinity requirements. For details on this, see comments in Q14. The PCA definition has a specific problem however. It essentially places a requirement inside a definition. The implicit requirement is that a BES Cyber Asset cannot share CPU/memory with a non-BCS of the same impact rating or a Protected Cyber Asset.. This is similar to the problem the current standards have with the definition of IRA having a requirement in it. If the SDT wishes this to be an auditable requirement, they should place the requirement within the standards and not within the glossary of terms.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
Please see the response in Q14.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment
ACES agrees with the added and modified terms except where noted in the responses to the questions in this comment form.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment
GSOC supports the majority of the revisions subject to its comment on particular definitions provided herein.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	

Comment
We agree with the new definitions of VCA, SCI and Management Interface, but disagree with the language in the definitions. We disagree with the changes to the definitions of CA, ESP, ERC, EAP , IRA and CIP System. See our proposed changes to the new and existing definitions and rationale for the disagreement in Q1.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment
Agree with the new and revised definitions short of the SCI definition.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3	
Answer	Yes
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

We agree with the new definitions of VCA, SCI and Management Interface, but disagree with the language in the definitions. We disagree with the changes to the definitions of CA, ESP, ERC, EAP , IRA and CIP System. See our proposed changes to the new and existing definitions and rationale for the disagreement in Q1.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	Yes
Document Name	

Comment

ACES agrees with the added and modified terms except where noted in the responses to the questions in this comment form.

AEPC signed on to ACES comments.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	

Comment
Suggest removing 'by a Responsible Entity' from the following definitions as it is implied or already stated in parent requirements. **BCS** - One or more BES Cyber Assets logically grouped to perform one or more reliability tasks for a functional entity, including Shared Cyber Infrastructure grouped in the BES Cyber System it supports. **CIP System** - A Cyber System identified as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset. **PACS -** Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) (including SCI grouped in the Physical Access Control Systems it supports) 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

Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	

Comment
The definitions on their own are acceptable.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	

Comment
AECI agrees with the new and revised several defined terms; however, the CIP standard are becoming increasingly difficult to understand and implement appropriately.

Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	

Response

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE recommends revising the definition of Shared Cyber Infrastructure (SCI) to indicate that SCI inherit the impact categorizations of all hosted VCAs. For example, the VCA definition states “A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure or a PCA.” Also, the BCA definition includes “…or Virtual Cyber Asset..” This could lead to interpretations that PCAs can host BCAs.

The proposed definition for Protected Cyber Asset is written in a way where Virtual Cyber Assets may be out of scope for security requirements despite being hosted on SCI that host critical systems, such as high impact BCS. These VCAs will hereafter be referred to as non-CIP VCAs. These non-CIP VCAs would not be required to be protected by an ESP pursuant to CIP-005 R1.1 and as such permitting any and all network traffic to them would be permissible. Additionally, as these non-CIP VCAs would not meet the definition of an applicable system in CIP-005 R1.1 then CIP-005 R1.3 would not apply and communications between the non-CIP VCAs and the SCI hosting them would be also permissible.

Texas RE notes that if there are security concerns related to network communications between CIP VCAs and their hosting SCI then these same concerns should be present for network communications between non-CIP VCAs and their hosting SCI. Texas RE proposes that the portion of the PCA definition “Share CPU or memory with any part of a BES Cyber System,” be revised to “Share CPU or memory with any part of a BES Cyber System or Shared Cyber Infrastructure,”

Texas RE seeks clarity around the description of the definition of Intermediate System in the Definitions and Exemptions technical rationale document. For the definition of Intermediate System, the “Definitions and Exemptions” technical rationale document states that requirement language has been removed from the definition. The specific example of where the Intermediate System must reside was provided, as the current definition of Intermediate System prevents Intermediate Systems from being located within ESPs. The technical rationale then goes on to say that such language has been moved to a mandatory requirement within CIP-005 R2. Texas RE believes this statement is a reference to CIP-005 R2.6.2.

Texas RE seeks clarity around this concept and proposes the following language for CIP-005 R2.6.3: Communications between Intermediate Systems and Applicable Systems of Part 2.1. must go through an EACMS enforcing an ESP.

Likes 0	
Dislikes 0	

Response

9. The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

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

Answer	No
Document Name	

Comment

A more detailed explanation of the rationale behind the addition addition of “discrete” needs to be provided for further clarification to enable an accurate response.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

No. Please see NRG’s response to question 2 for additional detail.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

No. Please see NRG’s response to question 2 for additional detail.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
CIP-002 should retain its focus on identification of BES Cyber Systems and the associated approval by the CIP Senior Manager.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy does not agree with proposed changes in CIP-002 and believe that the concept of SCI indenpednatly verified requires further clarity. We also support EEI comments on this question.	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	
Comment	
As further discussed in response to Questions 1 and 2, Duke Energy disagrees with the complexity added to the CIP-002 requirements. Based on our suggestion of the addition of an SCI Group defined term, simplified language proposed in response to Question 1 can be used. In Requirement 1.3, the comma following BCS introduces confusion and should be removed to be clear that the SCI clause follows onto the identify clause, and is not a requirement for a separate/additional list of assets that contain SCI supporting low BCS. Alternatively, bulleting the requirement after “asset that contains:” may be clearer. Changes to the Attachment 2 criteria 2.1 to incorporate the term “discrete” lose the context of the original RFI; if the SDT retains the new “discrete shared” language, a comma should be inserted between these terms, and clarification should be provided in the technical rationale to carry forward the clarification provided in the RFI. Additionally, the SCI bullet appears to exclude the possibility of independently identifying SCI at Generation facilities. If	

this was the SDT's intent, justification should be provided that explains why this option is not available to this facility type under section 2.1. Finally, Section 2.2 generally follows the same format as section 2.1 but was not given the second bullet related to SCI; was this intentional? If so, it would be helpful to provide explanation in an appropriate document.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
While mostly in agreement, please see our comments above responding to question #1.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	

AZPS agrees with EEI's comments around the concern that both data communication links and communication networks should be exempt. AZPS asks the SDT to explain why they are now excluding communications networks.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

The CIP-002 should maintain a section on BROS that establish the relationship with the BCS

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

The first draft contained the weighting to determine if a TOP Control Center met the medium impact criteria from CIP-002-6. The second draft reverted back to CIP-002-5.1a's criteria 2.12's language without informing the industry. While there is a new project to "study" the impacts to the BES with this change further delaying smaller entities compliance burden relief, it was not made clear to industry CIP-002's language was being reverted back under this project and was not shown as a change/redline from the first or redlined in the second draft which is highly misleading. If it is possible to incorporate other projects modifying other CIP standards into this project, why not the approved CIP-002-6 and complete the study at a later time?

AEPC has signed on to ACES comments.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Several of the terms and their usage, especially SCI, lends ambiguity with their use in the Standards. Further clarifications and refinements of the terms should be given attention.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE does not agree with the proposed changes to the 4.2.3.2. Exemption because in the “Lessons Learned CIP Version 5 Transition Program CIP-002-5.1: Communications and Networking Cyber Assets” issued by NERC, “study participants [in the Implementation Study] made a distinction between devices facilitating network communication locally for the BES Cyber Systems and those facilitating network communication external to the BES Cyber System or Facility. Entities determined network devices used only for external communication were out of scope in association with the high or medium impact BES Cyber System.” The “Lessons Learned CIP Version 5 Transition Program CIP-002-5.1: Communications and Networking Cyber Assets” was authorized by the Standards Committee on October 29, 2015 and is “ERO Enterprise – Endorsed Implementation Guidance.” However, it is still not in the standards and auditors can only go by the standards and not “Lesson Learned” documents.

The “between discrete ESPs” exemption is too narrow; all Cyber Systems used only for external communication need to be exempt, not just those between discrete ESPs. The reason is that there are instances when the same Cyber Systems can be used between two discrete ESP and between an ESP and non-ESP site. In one instance the Cyber Systems are exempt, in the other they are not, even though it is the same equipment performing the same function.

This narrow exemption has the potential of pulling Cyber Systems used for only external network communications into scope. Entities may have to bring telecommunication sites into compliance, which could mean additional costs, physical and electronic controls that would otherwise not be needed, and possibly more staff to produce and maintain the documentation required for compliance. This could create a situation where an Entity may have to choose a leased network over a private network due to the leased network being exempt even though it performs the same function as a private system.

Private systems are usually more reliable than leased systems, so overall the BES would be less reliable when using a leased system which is directly opposite of the purpose of the NERC standards. Private systems should be encouraged and exempting all Cyber Systems used only for external communications would do that.

CEHE proposes the following:

“4.2.3.2. Cyber Systems used only for external network communication between assets, or one or more geographic locations.”

Likes 0	
Dislikes 0	

Response
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment
NCPA does not support the modified language in CIP-002. How SCI is to be independently identified is not clear.

Likes 0	
Dislikes 0	

Response
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment
SIGE does not agree with the proposed changes to the 4.2.3.2. Exemption because in the “Lessons Learned CIP Version 5 Transition Program CIP-002-5.1: Communications and Networking Cyber Assets” issued by NERC, “study participants [in the Implementation Study] made a distinction between devices facilitating network communication locally for the BES Cyber Systems and those facilitating network communication external to the BES Cyber System or Facility. Entities determined network devices used only for external communication were out of scope in association with the high or medium impact BES Cyber System.” The “Lessons Learned CIP Version 5 Transition Program CIP-002-5.1: Communications and Networking Cyber Assets” was authorized by the Standards Committee on October 29, 2015 and is “ERO Enterprise – Endorsed Implementation Guidance.” However, it is still not in the standards and auditors can only go by the standards and not “Lesson Learned” documents. The “between discrete ESPs” exemption is too narrow; all Cyber Systems used only for external communication need to be exempt, not just those between discrete ESPs. The reason is that there are instances when the same Cyber Systems can be used between two discrete ESP and between an ESP and non-ESP site. In one instance the Cyber Systems are exempt, in the other they are not, even though it is the same equipment performing the same function. This narrow exemption has the potential of pulling Cyber Systems used for only external network communications into scope. Entities may have to bring telecommunication sites into compliance, which could mean additional costs, physical and electronic controls that would otherwise not be needed, and possibly more staff to produce and maintain the documentation required for compliance. This could create a situation where an Entity may have to choose a leased network over a private network due to the leased network being exempt even though it performs the same function as a private system. Private systems are usually more reliable than leased systems, so overall the BES would be less reliable when using a leased system which is directly opposite of the purpose of the NERC standards. Private systems should be encouraged and exempting all Cyber Systems used only for external communications would do that. SIGE proposes the following:

“4.2.3.2. Cyber Systems used only for external network communication between assets, or one or more geographic locations.”	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	
It is unclear what “independent SCI supporting any part of the high impact BCS…” is referring to.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
As noted in the answer to Question #1, Texas RE recommends the language require identification of all BCS, as well as their associated EACMS, PACS, and PCAs. Absent that change, Texas RE recommends the SDT review Requirement R1 for logical flow. The proposed Requirement R1 language instructs registered entities to identify each BCS as either a BCS or as a BCS and independent SCI. Texas RE notes that it is not possible to identify a BCS as an independent SCI. If the system is a BCS then it must be identified as a BCS. The SDT could consider revising the language to: 1.1. Per Attachment 1, Section 1: 1.1.1. Identify each high impact BCS; and 1.1.2. Identify each independent SCI supporting any part of the high impact BCS or its associated EACMS, PACS, or PCAs. 1.2. Per Attachment 1, Section 2:	

1.2.1. Identify each medium impact BCS; and;

1.2.2. Identify each independent SCI supporting any part of the medium impact BCS or its associated EACMS, PACS, or PCAs.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI Comments

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

We support NPCC TFIST's comments as found below:

Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain.

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI?

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
In support of NPCC RSC comments. Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain. Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI? Request correction of typo in R2 from the beginning “Each” to “The” Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI? The current wording creates more questions than answers. We suggest being more precise. See comments detailed in question one.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

"SCI independently identified" is frequently used throughout VSL in CIP-002, and "independent SCI" is used in the requirements. These phrases are not broadly understood and the intent needs to be clarified. In addition, AEP recommends SDT to add clarifying language to allow for the identification of both physical and virtual systems as EACMS, PACS and PCAs under CIP-002 as noted in response to Question #1.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The concept of *independent SCI* needs to be defined as this leaves it wide open to interpretation for what it is and where it might exist. The SDT also needs to consider defining terms vBCA and vBCS, this may help to provide clarity to the industry.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment
We disagree with CIP-002 changes. CIP-002 R1 requirements should be restored and all other SCI language in CIP-002 Attachment 1 should be removed based on our comments in Q1.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain. Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI? Request correction of typo in R2 from the beginning “Each” to “The” Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI? The current wording creates more questions than answers. We suggest being more precise. See comments detailed in question one.

Likes 0	
Dislikes 0	

Response

Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	No
Document Name	

Comment
Recommend including the definition within the text, or make a statement in the text directing to the definition in the definition list.

Likes 0	
Dislikes 0	

Response
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response
Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment
Remove the following phrases: from the second bullet on R1.1: “or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)” and from the second bullet on R1.2: “or its associated EACMS, PACS or PCAs.” These are expanding the scope of the CIP-002 identification and CIP Senior Manager approval, and identification of these associated with SCI will create confusion since these do not have to be identified in CIP-002 if they are not associated with SCI. On Attachment 1, under the medium impact rating criteria 2.1, to clarify the second bullet, change it to begin: “Any SCI supporting BCS that could, within 15 minutes, adversely impact….” (Delete “(which must be included in a shared BCS),” “one or more” and “together.”

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ISO-NE requests that the terms "high", "medium" and "low" used for impact ratings in the proposed CIP-002-7 be capitalized consistent with the rest of the CIP standards.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI?

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	No
Document Name	

Comment

Remove the following phrases: from the second bullet on R1.1: “or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)” and from the second bullet on R1.2: “or its associated EACMS, PACS or PCAs.” These are expanding the scope of the CIP-002 identification and CIP Senior Manager approval, and identification of these associated with SCI will create confusion since these do not have to be identified in CIP-002 if they are not associated with SCI.

On Attachment 1, under the medium impact rating criteria 2.1, to clarify the second bullet, change it to begin: “Any SCI supporting BCS that could, within 15 minutes, adversely impact….” **Delete** - “which must be included in a shared BCS,” “one or more,” and “together.”

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Please see our comments above responding to question #1.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
We disagree with CIP-002 changes. CIP-002 R1 requirements should be restored and all other SCI language in CIP-002 Attachment 1 should be removed based on our comments in Q1.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
• CIP-002 should include clarification for Cyber Assets with ERC that communications are converted serial needs to identify the risk to be mitigated applying the additional controls of ERC. ○ Entities are concerned many new CIP identified Cyber Asset using serial will come into scope requiring PSP controls and Password changes every 15 months.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
The first draft contained the weighting to determine if a TOP Control Center met the medium impact criteria from CIP-002-6. The second draft reverted back to CIP-002-5.1a's criteria 2.12's language without informing the industry. While there is a new project to "study" the impacts to the BES with this change further delaying smaller entities compliance burden relief, it was not made clear to industry CIP-002's language was being reverted back under this project and was not shown as a change/redline from the first or redlined in the second draft which is highly misleading. If it is possible to incorporate other projects modifying other CIP standards into this project, why not the approved CIP-002-6 and complete the study at a later time?	
Likes 0	
Dislikes 0	
Response	

Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	

Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain.

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI?

Likes 0	
Dislikes 0	
Response	

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	

<duplicate>

Likes 0	
Dislikes 0	
Response	

Maggy Powell - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	

The modifications to CIP-002 are complex and include a number of new terms and concepts. For example, AWS supports the SDT’s addition of requirements for Management Interfaces, but Management Interfaces are not required to be identified in CIP-002. CIP-002 requires the identification of SCI and EACMS, not the associated Management Interface. This situation also occurs with Intermediate Systems under the currently enforceable

Standards and has been problematic. The embedded classifications increase the opportunity for compliance violations and security oversights. AWS suggests including those terms directly in CIP-002 for clarity.

It would be helpful if the SDT provided in Implementation Guidance a logic diagram depicting how the device classifications and embedded definitions like Management Interface and CIP System can be applied.

Lastly, the SDT has been clear that this project focuses on on-premise virtualization, however, many virtualization concepts could be interpreted as being related to cloud computing technologies. AWS suggests explicitly stating that the Standards do not apply to cloud within the Applicability section of CIP-002. If these updated Standards do not apply to cloud, it should be obvious to the reader.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers this additional comment:

- Please see the ERCOT comments provided in Question 1.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI notes significant improvements to CIP-002 but asks for additional clarity for the following:

1) “SCI independently identified” is frequently used throughout CIP-002. This phrase is not broadly understood and the intent needs to be clarified.

2) In EEI’s comments to the previous draft of CIP-002, we expressed concern regarding the proposed removal of communications networks from the Exemption Section of the previous draft, noting that both data communication links and communication networks should remain exempt. Nevertheless, this change remains in Draft 2 and EEI seeks clarification why communications networks remain excluded from the Exemptions section in this proposed draft of CIP-002.

3) EEI recommends modifying 4.2.3.2 to align with endorsed ERO General Implementation Guidance titled “CIP Version 5 Transition Program, CIP-002-5-1: Communications and Networking Cyber Assets” dated October 6, 2015. EEI suggests the following:

4.2.3.2 Cyber Systems associated with:

4.2.3.2.1 Communication and networking devices between discrete Electronic Security Perimeters (ESP), and Cyber Systems associated with external communication to one or more geographic locations.” or

4.2.3.2.2 Non-routable communication externally directed between an ESP and one or more other geographic locations. or

4.2.3.2.3 Non-routable communication externally directed between BCS and one or more other geographic locations.

4) The inclusion of EACMS, PACS and PCAs seems redundant and possibly unnecessary in both the second bullet of R1.1 and the second bullet of R1.2. If this is an intentional, EEI request clarification within the Technical Rationale explaining the purpose of including of EACMS, PACS and PCAs.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

The requirement requires the identification of BCS as either “including any supporting SCI as part of the BCS” or with “independent SCI supporting any part of the high impact BCS or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).” This does not allow for the identification of BCS independent of having SCI, and therefore doesn’t account for non-virtualized environments.

The requirements and measures of CIP-002 do not sufficiently detail what is required to demonstrate compliance. The requirements are to create a list that identifies “each [BCS] as either” including supporting SCI or having independent SCI. However, the independent SCI details an association to EACMS, PACS, PCA. The requirement expects an identification of “BES Cyber Systems” but the sub-bullets imply an expectation to identify SCI and corresponding asset/system classifications. The measures and technical rationale provide no additional clarity other than creating lists. Is the expectation to simply provide identification that the identified BCS either include SCI or are supported by SCI (e.g. Yes/No or Checkbox), or is the expectation to explicitly identify and categorize SCI that meet this criteria (e.g. “1.) ABC High Impact BCS; 2.) CDE High Impact EACMS SCI”). If the expectation is to classify SCI, what should be the approach for classifying SCI that supports multiple classifications (e.g. EACMS and PACS)? As mentioned in Comment for #2 above, more clarity regarding grouping SCI could be beneficial as well.

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No

Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Remove the following phrases: from the second bullet on R1.1: “or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)” and from the second bullet on R1.2: “or its associated EACMS, PACS or PCAs.” These are expanding the scope of the CIP-002 identification and CIP Senior Manager approval, and identification of these associated with SCI will create confusion since these do not have to be identified in CIP-002 if they are not associated with SCI. On Attachment 1, under the medium impact rating criteria 2.1, to clarify the second bullet, change it to begin: “Any SCI supporting BCS that could, within 15 minutes, adversely impact….” (Delete “(which must be included in a shared BCS),” “one or more” and “together.”	
Likes 0	
Dislikes 0	
Response	

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	

Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain. Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI? Request correction of typo in R2 from the beginning “Each” to “The” Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI? The current wording creates more questions than answers. We suggest being more precise. See comments detailed in question one.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes the proposed revisions to Medium Impact Criterion 2.1 are confusing, particularly the parenthetical note in the second bullet that SCI “…must be included in a shared BCS” in order to potentially meet this criterion. If N&ST’s understanding of the SDT’s intentions regarding SCI, namely, that a Responsible Entity has the option of either including an SCI in a BCS (or an EACMS or a PACS) or identifying it as “independent” but supporting	

one or more BCS, EACMS, or PACS is correct, then we believe the second bullet, as written, is unnecessary. However, “independently identified” SCI that support BCS that meet Criterion 2.1 should be accounted for.

N&ST also believes the SDT should address the fact that Criteria 2.1 and 2.2, although ostensibly similar, are not consistent with each other: Criterion 2.2, as proposed, makes no mention of SCI at all.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The IRC SRC requests the SDT clarify why the terms “High Impact,” “Medium Impact” and “Low Impact” are capitalized in some instances while in other instances; e.g. Parts 1.1, 1.2 and 1.3, lower case is used. Is there a difference? If so, please explain. If not, the IRC SRC recommends the SDT standardize the capitalization treatment of “High Impact,” “Medium Impact” and “Low Impact” throughout.

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCS/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet under 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact assets could be consolidated into a Medium Impact asset due to shared SCI?

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Chelan approves of the revisions to CIP-002 but suggests clarification be made per comments for Q2.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
The draft CIP-002-7 standard now allows the Responsible Entity to identify SCI in the overall BCS or to identify them independently, it also requires the identification of SCI that supports EACMS, PACS, or PCAs. This gives Regional Entity enforcement staff the ability to identify noncompliance in a single requirement for a missed (SCI based) EACM, PACS, or PCA; rather than identifying all applicable requirements for a missed EACMS, PACS, or PCA.	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
We support these approach used for these changes once acceptable definitions are in place.	
Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
However while the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the proposed changes to the NERC glossary of terms. BC Hydro does not agree with the 'as is' state of the SCI definition proposed in this project comment/ballot submission.	
Likes 0	
Dislikes 0	
Response	

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
While mostly in agreement, we disagree with the SCI language and it should be removed from CIP-002.	
Likes 0	
Dislikes 0	
Response	

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC can support the changes to CIP-002 subject to ensuring the consistent identification of and reference to SCI.	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
A long standing “error” appears to remain in the High VSL for R1, where it states “For Responsible Entities with a total of 100 or fewer high or medium impact and BCA, more than 10 but less than or equal to 15 identified BCA have not been categorized or have been incorrectly categorized at a lower category” where Medium and Severe mention “BCS” instead of “BCA” This is the only mention of BCA in the VSL. It appears as though the latest modifications only replaced definitions and did not correct this error.	
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 generally agrees with the proposed changes to CIP-002 but with these suggestions for improvement. For R1.1 it would be clearer if it said "identify each high impact BCS as either of the following, if any, at each asset." The same for R1.2, "identify each medium impact BCS as either of the following, if any, at each asset." Both high and medium impact are clearly identified, and it does not imply that all BCS within an asset are of the same impact level. In addition, we suggest that CIP-002 not imply any process steps as identification methods vary within differing environments. Keep CIP-002 R1 as results-oriented as it has always been. We suggest capturing the options for SCI identification within the relevant definitions (as it currently is in the SCI proposal) and keep CIP-002 as close to the version 5.1a language as possible.	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Recommend spelling out "Shared Cyber Infrastructure" within CIP-002 standard text	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	

Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	

10. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Dan Zollner - Portland General Electric Co. - 3

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Replacing "BES Cyber System" with "CIP System" in the proposed definition of ERC appears to expand the scope of ERC from what was previously in place and now would include remote routable connectivity to PACS or EACMS. PGE wonders if this was the drafting team's intent. If not, Portland General Electric Company believes the phrase "CIP System" in the proposed definition of ERC could be replaced with "BES Cyber System" to resolve the scope expansion.

Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Replacing "BES Cyber System" with "CIP System" in the proposed definition of ERC appears to expand the scope of ERC from what was previously in place and now would include remote routable connectivity to PACS or EACMS. PGE wonders if this was the drafting team's intent. If not, Portland General Electric Company believes the phrase "CIP System" in the proposed definition of ERC could be replaced with "BES Cyber System" to resolve the scope expansion.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	
Answer	No
Document Name	

Comment

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces, and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request the SDT correct the typographical error, “Systerms” in Part 2.6.2 Requirements

Request the SDT clarify whether Exemption 4.2.3.3, which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations,” exempts any entity including third parties?

Likes 0	
Dislikes 0	

Response

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

Comment

N&ST offers the following observations about the proposed changes to CIP-005:

> Regarding the statement in Requirement R1 Part 1.1 (“Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”), N&ST believes it is highly inappropriate to include such an explicit directive in a CIP Standard Requirement statement. Standard Drafting Teams have, in recent years, endeavored to make Requirements non-prescriptive. The should likewise be non-proscriptive. N&ST notes this proposed change seems to have been made in response to a concern about “logical isolation” that was expressed by a single individual, representing one organization, during the previous ballot’s comment period, which ended 3/22/2021. N&ST believes concerns about host-based firewalls may actually be moot, given the fact the SDT has dropped “logical isolation” and restored the better-defined “ESP.” However, if the SDT believes this prohibition should be put in writing, it should by all means be done, but in an implementation guide, not a Standard.

> N&ST believes Requirement R1 Part 1.2 (“Permit only needed and controlled communications to and from Management Interfaces,…”) should apply to SCI identified independently and to SCI that are grouped into BES Cyber Systems.

> N&ST believes Requirement R1 Parts 1.2 and 1.3 are largely redundant and should be combined.

> Regarding Requirement R2, Part 1.2, N&ST believes “Applicable Systems” should include EACMS inside an ESP, if any (there are such devices in practice today).

> N&ST recommends that the SDT “true up” the wording of Requirement R2 Part 2.5 and Requirement R3 Part 3.2, which both address disabling/terminating vendor remote connections, so that they both say the same thing.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Replacing "BES Cyber System" with "CIP System" in the proposed definition of ERC appears to expand the scope of ERC from what was previously in place and now would include remote routable connectivity to PACS or EACMS. PGE wonders if this was the drafting team’s intent. If not, Portland General Electric Company believes the phrase "CIP System" in the proposed definition of ERC could be replaced with "BES Cyber System" to resolve the scope expansion.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Overall comment: We suggest reviewing the word ‘’communications’’, it should be a bi-directional routable protocol or a routable protocol. Communication is too vague. One could imply that serial, layer 2 communication needs to be controlled. If the intent of the SDT is to broaden the scope, why keep the notion of bi-directional routable protocol or routable protocol.

Requirement 1.1 New concept is inserted “between intelligent electronic devices”, what is an intelligent electronic device? We propose the SDT to use Cyber Asset definition.

The note regarding Host-based firewalls, is in sync with the definition of ESP, except we don’t agree on imposing this limitation. Also, the firewall wording is not used in the language of the requirements, controlled communication is the usual wording. We suggest the removal of this note.

The requirement should use the same language that is used for the other requirements. Suggestion

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that Permits only needed and controlled communications and denies all other communications.

Requirement 1.2 We suggest reviewing the measure column. MPLS is mainly a WAN protocol. Also, a network switch enforces the VLAN concept so the network switch would be an SCI and EACMS? We suggest that the SDT review the mechanism permitting the control of communication. Someone could build a complete ecosystem with only a network switch (BCA is on VLAN 2 and the permitted users are on VLAN 2, the denied users are on VLAN 3, all of this is managed and controlled by a network switch, a switch this is virtualized.

Requirement 1.3 introductions of network communication. For some requirement, communication is the only word used (1.1, 1.2), we suggest that the SDT review the usage of the word ‘’network’’ and be uniform within all standards.

Requirement 1.4: No Comments

Requirement 1.5 version 6 of this requirement is only applicable to BCA and PCA, in this version the SDT as added PACS hosted on SCI; and EACMS hosted on SCI, and SCI identified independently supporting an Applicable System above. One could understand why the SCI is part of the applicable systems but why did the SDT target PACS and EACMS. We suggest to the SDT to remove PACS and EACMS. Also the line “SCI identified independently supporting an Applicable System above” should be replaced by the usual language used throughout the requirements, i.e.” SCI identified independently supporting an Applicable System from Part 1.1.” Clarification to that sentence would also be welcome, are they “SCI identified independently” or are they “SCI that is identified to be supporting independently an Applicable System”.

Requirement 1.6, this requirement is valid in the context of the old ESP definition. In the context of the suggested definition, this is an additional requirement resulting in a burden for the entity. The SDT should evaluate the possibility of enforcing the ESP controls (permitted communication and malicious communications) directly on the cyber asset itself, an EACMS wouldn’t be required. The BCA, PCA, EACMS, PACS, SCI could have their own controls (host firewall, host IDS, Host Endpoint controls).

Requirement 2.1 We suggest reviewing the Applicable column

EACMS that enforces an ESP for the Applicable Systems in Part 1.1.

This is an additional requirement resulting in an additional burden for the entity.

SCI identified independently supporting an Applicable System above

We suggest the normal wording (SCI identified independently supporting an Applicable System from Part 1.1.

Increase in the need for Intermediate System (EACMS used for the ESP, SCI).

Requirement 2.2 No Comments

Requirement 2.3 No Comments

Requirement 2.4 We suggest the SDT normalize the wording, ‘’from SCI identified independently supporting an Applicable System above’’ to ‘’SCI identified independently supporting an Applicable System from Part 1.1’’.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn’t have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.5 We suggest the SDT normalize the wording, ‘’from SCI identified independently supporting an Applicable System above’’ to ‘’SCI identified independently supporting an Applicable System from Part 1.1’’.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn’t have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.6. Requirement 2.6.1 is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization or consolidating services like databases or web applications. We suggest the SDT review their objectives and how to implement them. The reference to Part 2.1 in 2.6 can also be confusing for the requirement, does the restriction in CPU and memory also apply to the SCI in 2.1 or only to the Intermediate Systems.

Requirement 2.6.2 should use the same language that is used for the other requirements. Suggestion

Permit only needed and controlled communications and denies all other communications between Intermediate Systems and Applicable Systems of Part 2.1.

Reference 2.6.1, Restrict VCAs of Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI

Reference 2.6.2. Permit only needed and controlled communications between Intermediate Systems and Applicable Systems of Part 2.1.

Requirement 3 Is this a new requirement part of the SAR?

Also, requirement 2.4 and Requirement 2.5 doesn’t mention the ERC criteria for the Medium Impact BES Cyber Systems, yet requirements 3.1 and 3.2 mention the ERC criteria. This will increase the burden on the entities. We suggest the SDT review the scope and criteria.

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Remove Intermediate Systems from the applicability for 2.1 to permit authorized IRA through an Intermediate System (on the clean version).

R1.1 – The last sentence in the requirement is prescriptive and would be more appropriate in the technical rationale document. Consider removing this and moving it to TR: “Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

R2.1 – Revise as follows to improve readability - Permit authorized IRA to Applicable Systems only through an Intermediate System.

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

Agree with change to CIP-005. Do not agree with Glossary of Terms, especially new ERC Definitions in NERC Glossary of terms.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI generally agrees with many of the proposed NERC Glossary terms, but we also identified a number of proposed terms that remain a concern. EEI is specifically concerned with the phrase “SCI identified independently”, which is not widely understood and needs to be clarified. For this and the following concerns we cannot support the proposed changes at this time. Requirement R1, subpart 1.4 may not fully cover the requirements set forth in CIP-006, Requirement R1, subpart 1.10. Associated PCAs are not included within subpart 1.4 but were specifically identified in CIP-006, subpart 1.10. This should be addressed or more clearly explained.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC believes the SDT is close, however, we have concerns there could be unintended consequences with CIP-005 due to the changes to the ESP and IRA definitions as well as the newly proposed Management Interface definition. Additionally, please consider incorporating the routability aspect back into the ESP definition to clarify scope.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers these additional comments:.

- Please see the ERCOT comments provided in Questions 3 through 5 above.
- Please clarify the statement at the end about host-based firewalls in Part 1.1.

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 disagrees with the applicability within R2. In R2.1, each Intermediate System is itself the object of the Intermediate System requirement, creating a hall of mirrors. Each Intermediate System is also an “EACMS that enforces an ESP”; it is an EACMS that enforces “policies or configuration” that “control communications”. See our fuller explanation of EACMS issues in Q14. In addition, there is an applicability difference between the clean and redline posted versions.

In addition, R2.6.2 points to the Applicable Systems of Part 2.1 as its applicability, however Part 2.1 includes the firewall (EACMS enforcing an ESP). We suggest R2.6.2 applicability should actually refer to Part 1.1, where only the BCS and the PCAs are in scope. That firewall (EACMS enforcing an ESP) is where one would implement R2.6.2, not the object of R2.6.2. Additionally, R2.6.2 has a spelling error (Systerms).

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	

The SDT is using the update to the definition as a mechanism to support zero-trust models, but the existing ESP definition does not preclude a Responsible Entity from applying the concept of zero-trust to its environment(s) in addition to its traditional ESP. The proposed modification does not obligate a Responsible Entity to adopt additional security controls.

The statement in the Definitions and Exemptions Technical Rationale, “[i]n these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS and nothing on the network is trusted for unrestricted communications,” could be interpreted as meaning that traditional ESP-based perimeter security is not necessary or required. A Responsible Entity may choose to adopt a traditional ESP model, or a zero-trust model, without considering the benefits of a defense-in-depth approach that leverages both traditional perimeter-based security and zero-trust concepts.

AWS proposes the following language, “The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol that includes a set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.”

Detailed implementation guidance is necessary to support zero-trust and hybrid approaches.

AWS supports the implementation of zero-trust architectures in fulfilling the NERC CIP Standards, but is seeking clarity on the assertion that the use of configurations or policies in the modified ESP definition can reduce the burden of documenting ESPs in a zero-trust environment. As the ESPs implemented by a Responsible Entity become more granular in a zero-trust environment, the documentation needs to support each policy or set of policies applied seeming to increase the compliance documentation.

Likes 0	
Dislikes 0	
Response	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	

<duplicate>

Likes 0	
Dislikes 0	
Response	

Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Likes 0	
Dislikes 0	
Response	

Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	

David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	

OPG concurs with NPCC's RSC comments

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- IRA and ERC when converted from routable IP to serial must be clarified. The language, application of and illustrations need to clearer. Additional and better use cases should be provided to address serial connected Cyber Assets.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC generally agrees with the proposed revision to the term ESP, but is concerned that, despite those revisions, the term ESP is used inconsistently in CIP-005-8. As an example, the proposed language in CIP-005-8, R1.2 appears to have an inconsistency between the

requirement and the measures. Specifically, the requirement language does not explicitly require an ESP while the measure appears to require an ESP. This also calls into question the inconsistent use of ESP between R1.1 and R1.2/1.3 and between these requirements and R1.6.

With the proposed modifications to the ESP definition, to avoid any confusion, it is recommended that specific language providing for traditional ESP protection of Applicable Systems be referenced as an option for meeting these requirements. Finally, if such language is not revised, GSOC requests clarification as to whether R1.6 is or should be applicable to any systems that are protected or are providing protections under R1.2 and R1.3 where those protections are not formally identified as an ESP. Inclusion of language such as "or other system or ESP" in Requirement R 1.6 would eliminate any uncertainty regarding protection of the Applicable Systems.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We disagree with the changes in CIP-005.

Recommendations:

- For CIP-005 R1.1, we have provided recommendation in Q4.
- For CIP-005 R1.2 and R1.3, resulting from our proposed changes to the definition of SCI, BCA, EACMS, PACS and PCA, the devices containing Management Interface will be identified as BCA, EACMS, PACS or PCA, therefore CIP-005 R1.2 and R1.3 are no longer needed.
- For CIP-005 R1.4, we agree to moving the CIP-006 R1.10 to CIP-005 R1.4 that is the right spot.
- For CIP-005 R1.6, resulting from our proposed changes to the definitions, we suggest changing the Applicable Systems to the following:
- Electronic Access Points for High Impact BES Cyber Systems
- Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers
- EACMS that controls all communications to and from the BCS unless ESP model is used.
- For CIP-005 R2.1, it has a "hall of mirrors" issue since the Intermediate System requires another Intermediate System. Resulting from our proposed changes to the definitions, we suggest changing the Applicable Systems to the following:
- High Impact BES Cyber Systems and their associated PCA
- Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA
- EACMS that contains EAP

- EACMS that controls all communications to and from the BCS unless ESP model is used
- For CIP-005 R2.4 and R2.5, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-005 R2.6, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA. We haven't seen any problem for an Intermedium System to share resources with other types of CIP Cyber Assets.
- For CIP-005 R3.1 and R3.2, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

We also want to point out that CIP-005-8 R1 Part 1.1 specifically denies '*Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement*' which does not meet the objective based model that the standards are supposed to now be written to. This very specifically identifies a technology that cannot be used to meet the requirement. This statement appears to be in conflict with the Technical Rationale for the ERC term.

ERC is no longer based on 'external' being defined in terms of the ESP as ESPs are changing in light of Zero Trust models. Zero Trust will shrink ESP's over time to the smallest, most granular object possible including a single device or possibly to process or resource level on a device.

Question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Please see comments regarding new definitions for ESP and EACMS. We believe the standard should address multi-layered access controls where traditional ESP boundaries are deployed using traditional firewalls, in addition to zero trust or host-based solutions. The IRA requirements should not apply to individual BCAs or PCAs with host-based solutions when they are also inside an ESP controlled by a traditional firewall.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No

Document Name	

Comment

NERC Definition Changes -- Electronic Security Perimeter (ESP) - removed the routable protocol qualifier. Consider the following:

* The new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. It seems like a circular definition.

When looking at the definitions only, it appears to require serial connected Cyber Assets have an EACMS to protect their serial communication links, however they are not required to have an Electronic Access Point (EAP) as the EAP definition has a routable communication qualifier.

When assessing CIP-005-8 R1.1 the Requirements section qualifies ESPs are only required for Applicable Systems with routable protocols. It does not have a qualifier of ERC so if there is only ethernet within a system that never leaves an asset, an ESP is required even if you have no EAP. This is the same as V5 of the standards.

If a BCA has both serial and Ethernet communications that leave an asset, auditors could require an EACMS for serial connections because a BCA that has routable protocol leaving an asset is required to have an ESP, and an ESP is required to have an EACMS. The same BCA serial that would leave the asset would require an EACMS because the ESP definition does not exclude serial communication. Not sure what type of device a serial EACMS would be.

The SDT proposed definition creates ambiguity around serial communication configurations and whether they have to be documented as part of an ESP.

We recommend revising CIP-005-X R1 Part 1.1 to read:

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other commuincations. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement. Excluding:

* Time sensitive protection or control functions between intelligent electronic devices

* Cyber Asset to Cyber Asset serial communication not meeting the IRA definition

Additionally, question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	No
Document Name	

Comment

Remove Intermediate Systems from the applicability for 2.1 to permit authorized IRA through an Intermediate System (on the clean version).

R1.1 – The last sentence in the requirement is prescriptive and would be more appropriate in the technical rationale document. Consider removing this and moving it to TR: “Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

R2.1 – Revise as follows to improve readability - Permit authorized IRA to Applicable Systems only through an Intermediate System.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces, and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	

Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	

Comment
Remove Intermediate Systems from the applicability for 2.1 to permit authorized IRA through an Intermediate System (on the clean version). R1.1 – The last sentence in the requirement is prescriptive and would be more appropriate in the technical rationale document. Consider removing this and moving it to TR: “Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.” R2.1 – Revise as follows to improve readability - Permit authorized IRA to Applicable Systems only through an Intermediate System.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	

Comment
Regarding CIP-005 R1.3, PNM Resources disagrees with this requirement. The technical rational is to keep users on SCI from being able to manage the SCI.This can be done via CIP-005 R1.2 where only permitted communication is allowed. It may be possible that an entity has an administrator workstation that is also a BCA that can access both the data plane and management plane. CIP-005 R1.2 can restrict the network traffic to include the administrator workstation. In addition electronic access controls should be in-place on the Management Interface to only allow the appropriate administrators access to it. The prescriptive and broad ban of traffic from the data plan seems excessive. The separation occurs in cloud-based hosting because the hosting service is the administrator and the tenant is not. For on-premise that is not the case and the administrator and tenant are the same entity. Does the SDT intend that those with on-premise virtualization purchase other physical workstation to manage the SCI? We cannot simply virtualize a PCA on the SCI to manage the SCI as it would be forbidden. The technical rational also is a bit inconsistent with the actual requirement. “The intent is users of a BCS hosted on an SCI that is identified independently and hosting other VCAs of differing impact levels should be prevented from having any access to the Management Interface of the underlying SCI.” The technical rational also doesn’t look at the 2nd and 3rd bullets in the definition of Management Interface, but only the first. The CIP-005 R1.3 requirement eliminates all BCS regardless of hosting status from having access to the Management Interface of the underlying SCI. We believe the controls in CIP-005 R1.2 along with electronic access controls for Management Interfaces is enough to prevent unauthorized users from managing the SCI or the EACMS that enforces the ESP. However CIP-005 R1.2 doesn’t address Management Interfaces on stand alone devices like physical server’s lights-out management port. If the SDT intends to fully protect lights-out management ports on stand-alone physical devices then it needs to be placed in scope in CIP-005 R1.2.

Regarding R2.1 missing a space in “Requirements” between “only” and “through”	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Overall comment: We suggest reviewing the word ‘’communications’’, it should be a bi-directional routable protocol or a routable protocol. Communication is too vague. One could imply that serial, layer 2 communication needs to be controlled. If the intent of the SDT is to broaden the scope, why keep the notion of bi-directional routable protocol or routable protocol.

Requirement 1.1 New concept is inserted “between intelligent electronic devices”, what is an intelligent electronic device? We propose the SDT to use Cyber Asset definition.

The note regarding Host-based firewalls, is in sync with the definition of ESP, except we don’t agree on imposing this limitation. Also, the firewall wording is not used in the language of the requirements, controlled communication is the usual wording. We suggest the removal of this note.

The requirement should use the same language that is used for the other requirements. Suggestion

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that Permits only needed and controlled communications and denies all other communications.

Requirement 1.2 We suggest reviewing the measure column. MPLS is mainly a WAN protocol. Also, a network switch enforces the VLAN concept so the network switch would be an SCI and EACMS? We suggest that the SDT review the mechanism permitting the control of communication. Someone could build a complete ecosystem with only a network switch (BCA is on VLAN 2 and the permitted users are on VLAN 2, the denied users are on VLAN 3, all of this is managed and controlled by a network switch, a switch this is virtualized.

Requirement 1.3 introductions of network communication. For some requirement, communication is the only word used (1.1, 1.2), we suggest that the SDT review the usage of the word ‘’network’’ and be uniform within all standards.

Requirement 1.4: No Comments

Requirement 1.5 version 6 of this requirement is only applicable to BCA and PCA, in this version the SDT as added PACS hosted on SCI; and EACMS hosted on SCI, and SCI identified independently supporting an Applicable System above. One could understand why the SCI is part of the applicable systems but why did the SDT target PACS and EACMS. We suggest to the SDT to remove PACS and EACMS. Also the line “SCI identified independently supporting an Applicable System above” should be replaced by the usual language used throughout the requirements, i.e.” SCI identified independently supporting an Applicable System from Part 1.1.” Clarification to that sentence would also be welcome, are they “SCI identified independently” or are they “SCI that is identified to be supporting independently an Applicable System”.

Requirement 1.6, this requirement is valid in the context of the old ESP definition. In the context of the suggested definition, this is an additional requirement resulting in a burden for the entity. The SDT should evaluate the possibility of enforcing the ESP controls (permitted communication and

malicious communications) directly on the cyber asset itself, an EACMS wouldn't be required. The BCA, PCA, EACMS, PACS, SCI could have their own controls (host firewall, host IDS, Host Endpoint controls).

Requirement 2.1 We suggest reviewing the Applicable column

EACMS that enforces an ESP for the Applicable Systems in Part 1.1.

This is an additional requirement resulting in an additional burden for the entity.

SCI identified independently supporting an Applicable System above

We suggest the normal wording (SCI identified independently supporting an Applicable System from Part 1.1.

Increase in the need for Intermediate System (EACMS used for the ESP, SCI).

Requirement 2.2 No Comments

Requirement 2.3 No Comments

Requirement 2.4 We suggest the SDT normalize the wording, ''from SCI identified independently supporting an Applicable System above'' to ''SCI identified independently supporting an Applicable System from Part 1.1''.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn't have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.5 We suggest the SDT normalize the wording, ''from SCI identified independently supporting an Applicable System above'' to ''SCI identified independently supporting an Applicable System from Part 1.1''.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn't have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.6. Requirement 2.6.1 is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization or consolidating services like databases or web applications. We suggest the SDT review their objectives and how to implement them. The reference to Part 2.1 in 2.6 can also be confusing for the requirement, does the restriction in CPU and memory also apply to the SCI in 2.1 or only to the Intermediate Systems.

Requirement 2.6.2 should use the same language that is used for the other requirements. Suggestion

Permit only needed and controlled communications and denies all other communications between Intermediate Systems and Applicable Systems of Part 2.1.

Reference 2.6.1, Restrict VCAs of Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI

Reference 2.6.2. Permit only needed and controlled communications between Intermediate Systems and Applicable Systems of Part 2.1.

Requirement 3 Is this a new requirement part of the SAR?

Also, requirement 2.4 and Requirement 2.5 doesn't mention the ERC criteria for the Medium Impact BES Cyber Systems, yet requirements 3.1 and 3.2 mention the ERC criteria. This will increase the burden on the entities. We suggest the SDT review the scope and criteria.

Likes 0	
Dislikes 0	

Response

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

We disagree with the changes in CIP-005.

Recommendations:

· For CIP-005 R1.1, we have provided recommendation in Q4.

· For CIP-005 R1.2 and R1.3, resulting from our proposed changes to the definition of SCI, BCA, EACMS, PACS and PCA, the devices containing Management Interface will be identified as BCA, EACMS, PACS or PCA, therefore CIP-005 R1.2 and R1.3 are no longer needed.

· For CIP-005 R1.4, we agree to moving the CIP-006 R1.10 to CIP-005 R1.4 that is the right spot.

· For CIP-005 R1.6, resulting from our proposed changes to the definitions, we suggest changing the Applicable Systems to the following:

- Electronic Access Points for High Impact BES Cyber Systems
- Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers
- EACMS that controls all communications to and from the BCS unless ESP model is used.

· For CIP-005 R2.1, it has a “hall of mirrors” issue since the Intermediate System requires another Intermediate System. Resulting from our proposed changes to the definitions, we suggest changing the Applicable Systems to the following:

- High Impact BES Cyber Systems and their associated PCA
- Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA
- EACMS that contains EAP
- EACMS that controls all communications to and from the BCS unless ESP model is used

· For CIP-005 R2.4 and R2.5, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

· For CIP-005 R2.6, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA. We haven’t seen any problem for an Intermedium System to share resources with other types of CIP Cyber Assets.

· For CIP-005 R3.1 and R3.2, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

NERC Definition Changes -- Electronic Security Perimeter (ESP) - removed the routable protocol qualifier. Consider the following:

- The new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. It seems like a circular definition.
- When looking at the definitions only, it appears to require serial connected Cyber Assets have an EACMS to protect their serial communication links, however they are not required to have an Electronic Access Point (EAP) as the EAP definition has a routable communication qualifier.

o When assessing CIP-005-8 R1.1 the Requirements section qualifies ESPs are only required for Applicable Systems with routable protocols. It does not have a qualifier of ERC so if there is only ethernet within a system that never leaves an asset, an ESP is required even if you have no EAP. This is the same as V5 of the standards.

o If a BCA has both serial and Ethernet communications that leave an asset, auditors could require an EACMS for serial connections because a BCA that has routable protocol leaving an asset is required to have an ESP, and an ESP is required to have an EACMS. The same BCA serial that would leave the asset would require an EACMS because the ESP definition does not exclude serial communication. Not sure what type of device a serial EACMS would be.

o The SDT proposed definition creates ambiguity around serial communication configurations and whether they have to be documented as part of an ESP.

We recommend revising CIP-005-X R1 Part 1.1 to read:

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement. Excluding:

- Time sensitive protection or control functions between intelligent electronic devices
- Cyber Asset to Cyber Asset serial communication not meeting the IRA definition

We also want to point out that CIP-005-8 R1 Part 1.1 specifically denies '*Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement*' which does not meet the objective based model that the standards are supposed to now be written to. This very specifically identifies a technology that cannot be used to meet the requirement. This statement appears to be in conflict with the Technical Rationale for the ERC term.

ERC is no longer based on 'external' being defined in terms of the ESP as ESPs are changing in light of Zero Trust models. Zero Trust will shrink ESP's over time to the smallest, most granular object possible including a single device or possibly to process or resource level on a device.

Additionally, question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

• R1.6 – Minnesota Power believes that the requirement is ambiguous and could be interpreted as traffic is only required to be monitored entering or leaving an ESP, but it could also be interpreted as traffic must be monitored both entering and leaving an ESP.

• R2.1 - Minnesota Power believes the inclusion of “Intermediate Systems used to access Applicable Systems of Part 2.1” in the Applicable Systems section of Part 2.1 creates a recursive reference that will never resolve as it would require an Intermediate System be used to access another Intermediate System.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP in general agrees with the proposed changes to the NERC Glossary terms, except as indicated in our responses above.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment
In support of NPCC RSC comments. Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.” Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts? Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS. Request correction of the typo “Systerms” in Part 2.6.2’s Requirements Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties? Overall comment: We suggest reviewing the word ‘’communications’’, it should be a bi-directional routable protocol or a routable protocol. Communication is too vague. One could imply that serial, layer 2 communication needs to be controlled. If the intent of the SDT is to broaden the scope, why keep the notion of bi-directional routable protocol or routable protocol. Requirement 1.1 New concept is inserted “between intelligent electronic devices”, what is an intelligent electronic device? We propose the SDT to use Cyber Asset definition. The note regarding Host-based firewalls, is in sync with the definition of ESP, except we don’t agree on imposing this limitation. Also, the firewall wording is not used in the language of the requirements, controlled communication is the usual wording. We suggest the removal of this note. The requirement should use the same language that is used for the other requirements. Suggestion Applicable Systems connected to a network via a routable protocol must be protected by an ESP that Permits only needed and controlled communications and denies all other communications. Requirement 1.2 We suggest reviewing the measure column. MPLS is mainly a WAN protocol. Also, a network switch enforces the VLAN concept so the network switch would be an SCI and EACMS? We suggest that the SDT review the mechanism permitting the control of communication. Someone could build a complete ecosystem with only a network switch (BCA is on VLAN 2 and the permitted users are on VLAN 2, the denied users are on VLAN 3, all of this is managed and controlled by a network switch, a switch this is virtualized. Requirement 1.3 introductions of network communication. For some requirement, communication is the only word used (1.1, 1.2), we suggest that the SDT review the usage of the word ‘’network’’ and be uniform within all standards. Requirement 1.4: No Comments Requirement 1.5 version 6 of this requirement is only applicable to BCA and PCA, in this version the SDT as added PACS hosted on SCI; and EACMS hosted on SCI, and SCI identified independently supporting an Applicable System above. One could understand why the SCI is part of the applicable systems but why did the SDT target PACS and EACMS. We suggest to the SDT to remove PACS and EACMS. Also the line “SCI identified independently supporting an Applicable System above” should be replaced by the usual language used throughout the requirements, i.e.” SCI identified independently supporting an Applicable System from Part 1.1.” Clarification to that sentence would also be welcome, are they “SCI identified independently” or are they “SCI that is identified to be supporting independently an Applicable System”. Requirement 1.6, this requirement is valid in the context of the old ESP definition. In the context of the suggested definition, this is an additional requirement resulting in a burden for the entity. The SDT should evaluate the possibility of enforcing the ESP controls (permitted communication and

malicious communications) directly on the cyber asset itself, an EACMS wouldn't be required. The BCA, PCA, EACMS, PACS, SCI could have their own controls (host firewall, host IDS, Host Endpoint controls).

Requirement 2.1 We suggest reviewing the Applicable column

EACMS that enforces an ESP for the Applicable Systems in Part 1.1.

This is an additional requirement resulting in an additional burden for the entity.

SCI identified independently supporting an Applicable System above

We suggest the normal wording (SCI identified independently supporting an Applicable System from Part 1.1.

Increase in the need for Intermediate System (EACMS used for the ESP, SCI).

Requirement 2.2 No Comments

Requirement 2.3 No Comments

Requirement 2.4 We suggest the SDT normalize the wording, ''from SCI identified independently supporting an Applicable System above'' to ''SCI identified independently supporting an Applicable System from Part 1.1''.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn't have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.5 We suggest the SDT normalize the wording, ''from SCI identified independently supporting an Applicable System above'' to ''SCI identified independently supporting an Applicable System from Part 1.1''.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn't have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.6. Requirement 2.6.1 is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization or consolidating services like databases or web applications. We suggest the SDT review their objectives and how to implement them. The reference to Part 2.1 in 2.6 can also be confusing for the requirement, does the restriction in CPU and memory also apply to the SCI in 2.1 or only to the Intermediate Systems.

Requirement 2.6.2 should use the same language that is used for the other requirements. Suggestion

Permit only needed and controlled communications and denies all other communications between Intermediate Systems and Applicable Systems of Part 2.1.

Reference 2.6.1, Restrict VCAs of Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI

Reference 2.6.2. Permit only needed and controlled communications between Intermediate Systems and Applicable Systems of Part 2.1.

Requirement 3 Is this a new requirement part of the SAR?

Also, requirement 2.4 and Requirement 2.5 doesn't mention the ERC criteria for the Medium Impact BES Cyber Systems, yet requirements 3.1 and 3.2 mention the ERC criteria. This will increase the burden on the entities. We suggest the SDT review the scope and criteria.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Remove Intermediate Systems from the applicability for 2.1 to permit authorized IRA through an Intermediate System (on the clean version). R1.1 – The last sentence in the requirement is prescriptive and would be more appropriate in the technical rationale document. Consider removing this and moving it to TR: “Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.” R2.1 – Revise as follows to improve readability - Permit authorized IRA to Applicable Systems only through an Intermediate System.	
Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

There is still there is a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication, but have not adequately enforced protections to ensure that the ports are not used by malicious actors – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to ensure validity of communications to Applicable Systems.

CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters but no minimum level of encryption is required which could result in older less secure methods being used leaving the data at risk.

CIP-005-8 depends upon approved SCI terminology and other definitions associated with virtualization as a whole. Approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization.

Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

The definition for ESP remains incomplete. We would suggest altering the definition as follows: “A logical boundary defined by a set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System and that groups CIP Systems of the same or lower impact rating”

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

We support NPCC TFIST's comments as found below:

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	No
Document Name	

Comment

MEAG Power adopts the Southern Company comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

While the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the definitions associated with some of the proposed NERC Glossary terms per comments provided in this project comment/ballot submission.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE recommends that the SDT consider an approach by which SCI is “high watermarked” to whatever applicable systems they are hosting.

Texas RE is concerned that not requiring SCI hosting BCS to be categorized as BCS themselves will result in a reduced security posture for those SCI. A previous version of the Technical Rationale indicated that SCI would be sufficiently protected, stating “The SDT recognizes that SCI indeed has the same impact as a virtual BES Cyber Asset and even more so if hosting numerous BES Cyber Assets. For the first formal posting of all affected standards, the requirements for SCI will be equal to BCA and in fact be subjected to additional requirements due to its impact (e.g. CIP-005 R1 Part 1.6).” In this current posting, however, Texas RE noticed CIP-005 R1.1 and CIP-005 R1.4 do not include SCI within scope as applicable systems, which means SCI arguably may not fall within the full scope of the CIP standards.

Texas RE also notes that “Intermediate Systems use to access Applicable Systems of Part 2.1” are an applicable system of Part 2.1. CIP-005 R2.1 requires that IRA must go through an Intermediate System. This appears to require Registered Entities to use an Intermediate System (IS1) prior to accessing a separate Intermediate System (IS2) that will then be used to access other applicable systems, such as high or medium impact BCS. Texas RE inquires as to whether or not this is the SDT’s intent.

Likes 0	

Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

The proposed revised definition of IRA as written, Management Interfaces of SCI would appear to need to reside within an ESP and Management Interfaces of EACMS that enforce the ESP would also need to reside within an ESP. As a whole it is very difficult to understand the security objective. This seems very prescriptive, trying to introduce security that is perhaps outside the scope of virtualization.

SCI identified independently supporting an Applicable System. 1.1 - is communication protected both inbound and outbound or only inbound? 1.3 - isn't this the same as 1.2; if an entity is only permitting needed communications then wouldn't one be denying communications from high impact BCS and PCA?

In CIP-005 R1.2 it is not clear with “only needed and controlled communications.” Only needed communications seems clear but controlled communications does not seem clear. Is this referencing not routed traffic such as broadcast traffic?

For 1.4 SMUD would like to see "mitigate the risk to data traversing" instead of "Protect the data." This would allow for entities to use their own transport media rather than a third parties transport networks. Encryption should not be a required control in this environment where availability is the top priority. For CIP-005 R2.1 – An RE would need an intermediate system to access an intermediate system and also need an intermediate system to get to an EACMS that enforces and ESP?

It is unclear what a bi-directional routable protocol is. It seems that the definition itself would exclude serial devices that are being communicated to since technically the communication is uni-directional. A serial connection cannot have bi-directional routable communication using a routable protocol, this is wrong. There can be IRA, but there is no bi-directional communication using a routable protocol. Entities are forced to overlook the fact that this is technically not correct but continues to be misinterpreted to ensure that serial communication is kept in scope. SMUD does agree that this serial communication should be in scope, but changing the meaning of bi-directional routable protocol make it very difficult to understand from a networking perspective.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment
SIGE does not agree to the ESP definition as stated in SIGE's response to question 4. SIGE proposed the following definition for ESP: "A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System and that groups CIP Systems of the same impact rating." SIGE does not agree to the IRA definition as stated in SIGE's response to question 5. SIGE proposed the following definition for IRA: "A user initiated real-time electronic access by a person from outside of a Responsible Entity's Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) to a CIP System within the Responsible Entity's ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System's user interfaces."

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	

Comment
NCPA does not support the modified language in CIP-005. How SCI is to be independently identified is not clear.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	

Comment
CEHE does not agree to the ESP definition as stated in CEHE's response to question 4. CEHE proposed the following definition for ESP: "A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System and that groups CIP Systems of the same impact rating." CEHE does not agree to the IRA definition as stated in CEHE's response to question 5. CEHE proposed the following definition for IRA:

“A user initiated real-time electronic access by a person from outside of a Responsible Entity’s Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) to a CIP System within the Responsible Entity’s ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System’s user interfaces.”	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Several of the terms and their usage, especially SCI, lends ambiguity with their use in the revised CIP-005 Standard. Further clarifications and refinements of the terms should be given attention.	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
While mostly in agreement with the proposed changes, we note a possibility that with the revised ESP definition and revised verbiage of R1.1 that an interpretation could be made that an ESP is required around serial-only connections. Please revise requirement part verbiage accordingly to prevent this possible interpretation. Additionally, question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No

Document Name	
Comment	
Need clarification for IRA and ERC . See comments for questions 3 and 5	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
See response to question 3, 5, and 6	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Consider adding 'Virtual Cyber Asset' context to the EAP definition, just as has been added to the EACMS definition. This would allow for Virtual Cyber Asset based firewalls and virtual firewall appliances to have an identified EAP as well. The inclusion of 'Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement' is not consistent with the proposed ESP definition. Consider the following - **EAP -** A policy enforcement point or a Cyber Asset, Virtual Cyber Asset interface that allows routable communication to and from the BES Cyber System within an Electronic Security Perimeter. The language 'must be protected by an ESP that permits only…' used in Part 1.1 appears to be out of context for an ESP, as defined. Wouldn't it be an EACMS that is performing the electronic access control? This would be more consistent with the language use in the Applicable Systems of Part 1.6. Consider the following language -	

Applicable Systems connected to a network via a routable protocol must be (within an ESP and protected by an EACMS) ADD WORDS IN () that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices.

Specific to Part 1.2, the use of 'controlled' may create more ambiguity in meeting the security objective than intended. Also noting the use of 'needed communications' in Part 1.1, 'controlled communications' in Part 1.2 and 'network communications' in Part 1.3. Consider the following language –

Permit only needed and controlled communications to and from Management Interfaces, and deny all other communications.

Part 1.4, consider the use of 'electronic controls' to be consistent with the second bullet.

'Electronic controls that ensure confidentiality and integrity (such as encryption), or…'

Part 2.1, the use of 'Intermediate Systems used to access Applicable Systems of Part 2.1' as an Applicable Systems does not appear to be consistent with the ESP definition as IRA to an IS does not include an IS.

Part 2.2, consider changing 'client' to 'remote Cyber Asset' or 'remote client' to the requirement –

Protect the confidentiality and integrity (e.g., encryption) of IRA between the (remote) ADD WORK IN () Cyber Asset and the Intermediate System.

Part 2.6, the inclusion 'Intermediate Systems used to access Applicable Systems of Part 2.1' appears to create a hall of mirrors, meaning an Intermediate System used to access an Intermediate System.

Part 2.6.2, suggest removing 'controlled' and only using 'needed communications' as has been used in other parts.

Permit only needed (and controlled) DELETE WORDS IN () communications between Intermediate Systems and Applicable Systems of Part 2.1.

Likes 0	
Dislikes 0	

Response

Josh Johnson - Lincoln Electric System - 1

Answer	No
Document Name	

Comment

We agree with the changes to the standard, however, the potential clarity issues that arise from the definition changes of ESP (and subsequently an EACMS) may cause unintended scoping regarding Registered Entities BCS in the field. See question 4 for further explanation and alternative proposal.

Likes 0	
Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5

Answer	No

Document Name	
Comment	

NERC Definition Changes -- Electronic Security Perimeter (ESP) - removed the routable protocol qualifier. Consider the following:

- The new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. It seems like a circular definition.
- When looking at the definitions only, it appears to require serial connected Cyber Assets have an EACMS to protect their serial communication links, however they are not required to have an Electronic Access Point (EAP) as the EAP definition has a routable communication qualifier.
- When assessing CIP-005-8 R1.1 the Requirements section qualifies ESPs are only required for Applicable Systems with routable protocols. It does not have a qualifier of ERC so if there is only ethernet within a system that never leaves an asset, an ESP is required even if you have no EAP. This is the same as V5 of the standards.
- If a BCA has both serial and Ethernet communications that leave an asset, auditors could require an EACMS for serial connections because a BCA that has routable protocol leaving an asset is required to have an ESP, and an ESP is required to have an EACMS. The same BCA serial that would leave the asset would require an EACMS because the ESP definition does not exclude serial communication. Not sure what type of device a serial EACMS would be.
- The SDT proposed definition creates ambiguity around serial communication configurations and whether they have to be documented as part of an ESP.

We recommend revising CIP-005-X R1 Part 1.1 to read:

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other commuincations. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement. Excluding:

- Time sensitive protection or control functions between intelligent electronic devices
- Cyber Asset to Cyber Asset serial communication not meeting the IRA definition

We also want to point out that CIP-005-8 R1 Part 1.1 specifically denies '*Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement*' which does not meet the objective based model that the standards are supposed to now be written to. This very specifically identifies a technology that cannot be used to meet the requirement. This statement appears to be in conflict with the Technical Rationale for the ERC term.

ERC is no longer based on 'external' being defined in terms of the ESP as ESPs are changing in light of Zero Trust models. Zero Trust will shrink ESP's over time to the smallest, most granular object possible including a single device or possibly to process or resource level on a device.

Additionally, question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.

Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No

Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	
Comment	

For Part 1.1, we suggest including the word “directly” in this phrase “connected directly to a network” for absolute clarity that serial devices do not require an ESP, regardless of any upstream protections afforded by the newly proposed IRA definition.

We also suggest that Part 1.1 be modified to remove the host-based language due to proposed inclusion in glossary term as described in response to Question 4.

We suggest aligning the Applicable Systems language in (current) Part 1.4 and (current) Part 1.6 using reference back to Part 1.1 with additional “at Control Centers” qualifier.

We suggest placing the “ESP outside PSP” requirement as the new Part 1.6 so that dial-up and malicious communications requirements maintain their current part numbers. This minor change would allow for continuity of evidence references that would otherwise be confusing and burdensome.

Inclusion of the ESP reference in the malicious communication requirement may present challenges for Zero Trust environments where an application layer firewall or IDS cannot be applied between each ESP. Language such as the following would allow for more flexible implementations that still meet the security objective of this requirement: “Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP. Detection may occur at the boundary or as part of EACMS monitoring capabilities.”

Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	

Xcel Energy does not agree with the proposed changes in CIP-005. Independly identified SCI is listed throughout the applicable systems column and with our concern with the lack of clarity in Independly identified SCI, we can not support at this time.

While Xcel Energy does not support the approval of this Standard at this time, we do support other aspects in the modifications made as identified in EEI comments.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

See response to question #4.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

:No. Please see NRG’s responses to questions 4 and 7.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

No. Please see NRG's responses to questions 4 and 7.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

In Reference to CIP-005-8

No – As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture. I have a request for additional information from the Standards Drafting Team to get clarity.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

Chelan agrees in principle with CIP-005, but there is a major flaw in CIP-005 R2. CIP-005-8 R2.1 includes "Intermediate Systems used to access Applicable Systems of Part 2.1" as part of the Applicable Systems. This language indicates that an Intermediate System is required to access an Intermediate System. Is this a typo? If not, additional clarification is requested. This appears to create a hall of mirrors.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
CIP-005-8 R1 Part 1.6 proposes the following: Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP. In light of the new ESP definition, perhaps this requirement should state: Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving an applicable system. In the alternative, the new definition of ESP would need further refinement. CIP-005-8 R1 Part 1.4 is another example where the language of the requirement appears to be using the approved ESP definition from CIP V5.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	

Comment
Tacoma Power agrees with the proposed changes to the NERC Glossary terms. However, we identified the following improvements and minor corrections to the CIP-005 documentation: • Suggest simplifying the measures in CIP-005 R1 Part R1.1 by moving the following sentence into the opening statement: “that enforces an ESP electronic access control and logical isolation and documents the business need.” • In CIP-005 R2 Part 2.1, a space is needed between “onlythrough”. • In the clean version of CIP-005 R2 Part 2.1, the last statement in the Applicable Systems column, “Intermediate Systems used to access Applicable Systems of Part 2.1,” should be removed. • Correct typo in CIP-005 R2 Part 2.6.2: “Systerms” should be “Systems”.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	

Comment

SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
We support these approach used for these changes once acceptable definitions are in place.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS does not believe that Requirement R1.4 accounts for all of CIP-006, Requirement R1.10. There is a lack of associated PCAs in Requirement R1.4 that was contained within CIP-006 R1.10.	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

11. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

The changes to CIP-007 R1.1 and the conforming changes are appropriate. The new requirement CIP-007 R1.3 is too specific in requiring a specific technology be used. See comments in Q14 for comments on CIP-007 R1.3

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

See response to questions #1, #2, and #6.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy does not agree with the proposed changes in CIP-007. Independly identified SCI is listed throughout the applicable systems column and with our concern with the lack of clarity in Independly identified SCI, we can not support at this time.

While Xcel Energy does not support the approval of this Standard at this time, we do support other aspects in the modifications made as identified in EEI comments.

Likes 0	

Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
We support the proposed R1.3. We do not support the other changes to the standard. The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. It is unclear why R1.2 Applicable Systems now include “Non-programmable communications components located inside both a PSP and ESP” for both high and medium impact.	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
See response to question 3, 6, and 8	

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	No
Document Name	

Comment

AZPS does not agree with the proposed changes in Requirement 1.2 and would like clarification on what “non-programmable communications components located inside both a PSP and ESP”includes.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Need clarification for SCI “identify independently”. See comment for question 2.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	

Comment

The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. It is unclear why R1.2 Applicable Systems now include “Non-programmable communications components located inside both a PSP and ESP” for both high and medium impact. Lastly, question #11 begins by asking about the revised CIP-007 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-007.

We are concerned about revising the existing CIP standards to address virtual technologies. We recommend any necessary requirements pertaining to security controls around virtual cyber assets used for a CIP function be encoded in a new Reliability Standard. Please see our comment on this in response to question #14.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Several of the terms and their usage, especially SCI, lends ambiguity with their use in the revised CIP-007 Standard. Further clarifications and refinements of the terms should be given attention.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree to the Management Interface definition as stated in CEHE's response to question 6. CEHE proposes the following definition: "A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems."	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	

Comment
NCPA does not support the modified language in CIP-007. How SCI is to be independently identified is not clear.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment
SIGE does not agree to the Management Interface definition as stated in SIGE's response to question 6. SIGE proposes the following definition: "A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems."

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
While the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the SCI definition proposed in this project comment/ballot submission. Otherwise, the CIP-007 standard itself is largely unchanged and no other issues were identified.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No

Document Name	
Comment	

We support NPCC TFIST's comments as found below:

Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.”

Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency

Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.

Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

The modification to the definition to ERC brings serially connected OT Devices using a protocol-converter into scope for multiple CIP-007 requirements. In some instances, compliance with all the CIP-007 requirements would be impossible. The use of a protocol converter does not facilitate centralized logging, review, and alarming (based on events). It simply facilitates data acquisition and IRA to these devices. We suggest not revising the definition of ERC, leaving the concept of a protocol break in place and require the protocol converter to either be categorized as a BCA, PCA or EACMS (depending on the circumstance). The serial OT device could still utilize the proposed definition for IRA to be in scope for CIP-005.

Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	

OKGE supports EEI's comments.

Likes 0	

Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	

Comment
Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	

Comment
In support of NPCC RSC comments. Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.” Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity. Requirement 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA We do not understand the change from Where technically feasible, enable only logical network accessible ports (previous version) to Enable only network-accessible Internet Protocol (IP) ports (suggested version). The introduction of IP is limiting. SDT should try to use routable protocol, Enable only network-accessible routable protocol ports. Requirement 1.2 This new criteria for the applicable system, Non-programmable communication components located inside both a PSP and ESP is difficult to understand because the NERC CIP always treated cyber assets, the non-programmable were always excluded from the CIP standards. This is an increase in scope and doesn’t seem related to the virtualization project.

We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above.

Requirement 1.3 This requirement is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization. Thus, avoiding the sharing resources between non-CIP VCAs and CIP VCA doesn't offer any benefits versus the current version. We suggest that the SDT review their objectives and how to implement them.

Requirements 2, 3, 4, 5 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We disagree with the changes in CIP-007.

Recommendations:

· For CIP-007 R1.1 and R1.2, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

· For CIP-007 R1.3, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA.

· For CIP-007 R2.1, R2.2, R2.3 and R2.4, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

· For CIP-007 R3, R4, R5 and their Parts, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. It is unclear why R1.2 Applicable Systems now include “Non-programmable communications components located inside both a PSP and ESP” for both high and medium impact.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.”

Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency

Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.

Requirement 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

We do not understand the change from Where technically feasible, enable only logical network accessible ports (previous version) to Enable only network-accessible Internet Protocol (IP) ports (suggested version). The introduction of IP is limiting. SDT should try to use routable protocol, Enable only network-accessible routable protocol ports.

Requirement 1.2 This new criteria for the applicable system, Non-programmable communication components located inside both a PSP and ESP is difficult to understand because the NERC CIP always treated cyber assets, the non-programmable were always excluded from the CIP standards. This is an increase in scope and doesn’t seem related to the virtualization project.

We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above.

Requirement 1.3 This requirement is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization. Thus, avoiding the sharing resources between non-CIP VCAs and CIP VCA doesn’t offer any benefits versus the current version. We suggest that the SDT review their objectives and how to implement them.

Requirements 2, 3, 4, 5 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

R1.4 Applicablity is missing SCI that may be part of a BCS. As written, it implies that SCI as part of a BCS aren't subject to this requirement. Or is this an issue with clarity around CIP-002 or the actual definition? Is the idea the independently identified SCI is the only SCI with non-CIP Systems hosted on them. If so that needs to be made clear in CIP-002 or the definition. If not then the scope of R1.4 needs to include "SCI identified as part of a BES Cyber System, EACMS, or PACS" or possibly strike "identified independenty" so we get "SCI supporting:…"

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
The change to specification of "Internet Protocol ports" in proposed CIP-007-7 R1.1 supports technical restriction of protection to only a particular network technology. The prior language for CIP-007 R1.1 did not involve "Internet Protocol" ports and allowed for service identification to include one/more ports. ISO-NE requests either clarification of the intent regarding technical specification of networking technology for this case or reversion of the requirement language to support backward compatibility.	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 3	
Answer	No
Document Name	
Comment	
GRE agrees with the comments submitted by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

In support of IRC SRC/SWG.

Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.”

Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency

Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Please provide more clarity on Requirement 1.2

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We disagree with the changes in CIP-007.

Recommendations:

- For CIP-007 R1.1 and R1.2, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-007 R1.3, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA.

- For CIP-007 R2.1, R2.2, R2.3 and R2.4, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-007 R3, R4, R5 and their Parts, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

o CIP-007 R1 – Please confirm the P1.1 Logical ports justification and details for serially connected CIP Systems are excluded but expectation of the physical wiring will be required for P1.2?

o CIP-007 R4.2 – Please clarify the serial CIP System must now alert for failure of event logging.

o CIP-007 R5.6 – Please clarify a serial CIP System such as an RTU or Relay that was a BCA or PCA without ERC now with the proposed change requires the password change every 15 months?

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan

Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	
Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.” Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.	
Likes 0	
Dislikes 0	
Response	

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT supports the IRC SRC comments.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI supports many of the proposed NERC Glossary terms, however, concerns remain with those terms identified in our comments above. EEI also notes that the phrase “SCI identified independently” is unclear in its intent and needs to be clarified before EEI can support the revisions to CIP-007.	
Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No

Document Name	
Comment	
Agree with change to CIP-007. Do not agree with related NERC Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC. PJM requests additional clarity on what is considered a “non-programmable communication component”.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	

Comment

Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.”

Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency

Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.

Requirement 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

We do not understand the change from Where technically feasible, enable only logical network accessible ports (previous version) to Enable only network-accessible Internet Protocol (IP) ports (suggested version). The introduction of IP is limiting. SDT should try to use routable protocol, Enable only network-accessible routable protocol ports.

Requirement 1.2 This new criteria for the applicable system, Non-programmable communication components located inside both a PSP and ESP is difficult to understand because the NERC CIP always treated cyber assets, the non-programmable were always excluded from the CIP standards. This is an increase in scope and doesn’t seem related to the virtualization project.

We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above.

Requirement 1.3 This requirement is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization. Thus, avoiding the sharing resources between non-CIP VCAs and CIP VCA doesn’t offer any benefits versus the current version. We suggest that the SDT review their objectives and how to implement them.

Requirements 2, 3, 4, 5 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

N&ST believes Requirement R1 Part 1.3 (“Prevent the sharing of the CPU and memory,…”) should apply to SCI identified independently and to SCI that are grouped into BES Cyber Systems.

N&ST also believes Requirement R1 Part 1.3 should be slightly revised for better clarity. We suggest, “Prevent the sharing of the CPU, memory, and Management Interfaces of SCI with non-CIP Systems.”

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.”

Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency.

Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	Yes

Document Name	
Comment	
Duke Energy agrees with the proposed CIP-007 strategy and notes that several definition concerns are identified in response to other Questions.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Part 1.1, consider removing 'by the Responsible Entity' as it is already stated in R1, 'Each Responsible Entity shall…' Part 1.3, the use of 'Management Interfaces' in the requirement is redundant with the definition of SCI. Consider changing to the following - Prevent the sharing of the CPU and memory of Applicable Systems (Management Interfaces of SCI) DELETE WORDS IN () with non-CIP Systems.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
We support these approach used for these changes once acceptable definitions are in place.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes

Document Name	

Comment

ACES agrees with the changes made based on industry comments, but regarding R2, based on webinar and technical rationale documentation, dormant VCAs are not considered Applicable Systems until they become “active” instances again. How is this going to be handled if an entity’s SCI automatically spins up dormant VCA’s when needed, how would an entity track and document the controls necessary prior to being an active VCA? Allowing automatic remediation of non-responsive VCAs is a benefit to utilizing virtualization and could cause an entity to be out of strict compliance.

Also, wouldn’t a dormant instance previously a VCA, which could be a VCA in the future that has not been “connected” to the BCS for 30 consecutive days be considered a TCA? ACES feels like there needs to be VERY clear guidance on how to keep dormant VCAs compliant, that aren’t actually in scope when dormant and if dormant for greater than 30 days constitutes a VCA as a TCA. In our opinion an in scope VCA, dormant or not, should always remain in scope until retired. Virtualized environments are highly dynamic, thus the standards should have considerations for such capabilities.

AEPC has signed on to ACES comments.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	Yes
Document Name	

Comment

SDG&E supports EEI Comments

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	Yes
Document Name	

Comment

MEAG Power adopts the Southern Company comments.

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Although we agree with returning back to looking at ports and not just services the updated language uses the term “Internet Protocol (IP) Ports”. Under Internet Protocol (IP), the transport layers (e.g. TCP, UDP) create and maintain the ports for the underlying services. The Internet Protocol is the network layer, which uses the host address to communicate. Consider alternate verbiage.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	

Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports many of the proposed NERC Glossary terms, however, concerns remain with those terms identified in our comments above.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We support the proposed R1.3. The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. It is unclear why R1.2 Applicable Systems now include “Non-programmable communications components located inside both a PSP and ESP” for both high and medium impact.	
Likes 0	

Dislikes 0	

Response

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

Comment
ACES agrees with the changes made based on industry comments, but regarding R2, based on webinar and technical rationale documentation, dormant VCAs are not considered Applicable Systems until they become “active” instances again. How is this going to be handled if an entity’s SCI automatically spins up dormant VCA’s when needed, how would an entity track and document the controls necessary prior to being an active VCA? Allowing automatic remediation of non-responsive VCAs is a benefit to utilizing virtualization and could cause an entity to be out of strict compliance. Also, wouldn’t a dormant instance previously a VCA, which could be a VCA in the future that has not been “connected” to the BCS for 30 consecutive days be considered a TCA? ACES feels like there needs to be VERY clear guidance on how to keep dormant VCAs compliant, that aren’t actually in scope when dormant and if dormant for greater than 30 days constitutes a VCA as a TCA. In our opinion an in scope VCA, dormant or not, should always remain in scope until retired. Virtualized environments are highly dynamic, thus the standards should have considerations for such capabilities.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	

Comment
No comments

Likes 0	
Dislikes 0	

Response

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

Comment

Southern agrees with the proposed changes to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	
Document Name	

Comment

It is not clear what is meant by SCI identified independently supporting an Applicable System. The wording “identified independently” is not clear.

Likes 0	
Dislikes 0	

Response

12. The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Dan Zollner - Portland General Electric Co. - 3

Answer	No
Document Name	

Comment

Portland General Electric Company supports most changes, but has concerns regarding changes to the TCA definition and applicability language in R4. In the current CIP-010-2 Standard, R4 clearly limits scope to High Impact and Medium Impact BES Cyber Systems and their associated PCAs. The proposed modification to the Standard appears to only exclude Low Impact BES Cyber Systems and supporting SCI. This implies that EACMS and PACS may now also be in scope. Based on the proposed definition of TCA, any Cyber Asset or VCA that meets the first three qualifiers and is connected for 30 consecutive calendar days or less to any Shared Cyber Infrastructure (including SCI that is only supporting a PACS or EACMS) is in scope for R4. This appears to be a fairly significant change in scope. Portland General Electric Company wonders if this was the drafting team's intent. If not, changing "Shared Cyber Infrastructure" to "Shared Cyber Infrastructure supporting a BES Cyber System" may resolve this. Additionally, clearly identifying scope within the R4 language (i.e. high impact and medium impact BES Cyber Systems, associated Protected Cyber Assets, and supporting SCI) may reduce confusion about the applicability of R4.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

N&ST believes proposed changes beyond those needed for conformance:
Have little or nothing to do with virtualization,
Are unlikely to improve anyone’s cyber security posture,
Are outside the scope of the original 2016 SAR,
Are not addressed in any relevant FERC Order, and
Would be an unnecessary and unwelcome distraction for entities trying to adjust their CIP programs and documentation to accommodate new virtualization-related requirements.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5	
Answer	No
Document Name	
Comment	

Portland General Electric Company supports most changes, but has concerns regarding changes to the TCA definition and applicability language in R4. In the current CIP-010-2 Standard, R4 clearly limits scope to High Impact and Medium Impact BES Cyber Systems and their associated PCAs. The proposed modification to the Standard appears to only exclude Low Impact BES Cyber Systems and supporting SCI. This implies that EACMS and PACS may now also be in scope. Based on the proposed definition of TCA, any Cyber Asset or VCA that meets the first three qualifiers and is connected for 30 consecutive calendar days or less to any Shared Cyber Infrastructure (including SCI that is only supporting a PACS or EACMS) is in scope for R4. This appears to be a fairly significant change in scope. Portland General Electric Company wonders if this was the drafting team's intent. If not, changing "Shared Cyber Infrastructure" to "Shared Cyber Infrastructure supporting a BES Cyber System" may resolve this. Additionally, clearly identifying scope within the R4 language (i.e. high impact and medium impact BES Cyber Systems, associated Protected Cyber Assets, and supporting SCI) may reduce confusion about the applicability of R4.

Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Requirements 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above, SDT should be more precise. Requirement 1.1.5 (.1.5. Any security patches applied.) was removed, yet the measure “Documentation of authorization for cybersecurity patches implementation” was added as evidence of change authorization for security patches. Need for clarification as the change seems contradictory.

We suggest that the SDT review the wording of requirement 1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware; This requirement mention ‘’images’’, why not use the word ‘’container’’?

Requirement 1.2 The overall requirement is questionable. Enforcing restrictions on the sharing of CPU or memory between systems limits the possible gain of instating virtualization. Also following the new definition of ESP, the latter is enforced by an EACMS and not by the SCI. We suggest that the SDT reviews their objectives and how to implement them.

Requirement 1.3 To be coherent shouldn't this requirement refer also to 1.2. After all, the CPU and memory controls are CIP-007 and the ESP is CIP-005. Follow the same logic as 1.4, i.e. ‘’for each change to the items listed in Part 1.1 or Part 1.2’’.

Requirement 1.4 no comments

Requirement 1.5 Our understanding is that we don’t need to verify the source nor the integrity of the security patches any longer. Since CIP-007 Patch management does not include those checks, wouldn’t this be considered as neglecting a compliance sound practice? (To validate the security patches)? Is this the real intent of the SDT?

Requirement 2.1 no comments

Requirement 3.3 What does ‘’Prior to becoming a new Applicable System” means?

We suggest that the SDT defines ‘’becoming’’. Is the intent of the SDT to permit the creation of a virtual cyber asset on an SCI, this SCI being in a production environment? We suggest that the SDT review the usage of ‘’production environment’’ versus ‘’becoming’’.

There is a need for additional clarification for “same type” in “like replacements of the same type of Cyber System”. Is ‘’type’’ associated with the Cyber System definition?

Since the baseline configuration doesn’t exist anymore, what is the intent of the SDT with the usage of the word ‘’configuration’’? How does one entity define configuration?

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the SWG. PJM requests to further define firmware (ex: does include BIOS and UEFI?) and provide implementation guidance for application containers.	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	

The requirement to “Authorize changes to 1.1.5 Security patches applied” was removed per the Technical Rationale that these changes would be included to changes to OS/Firmware or software, which Entergy agrees. However, the measures were explicitly updated to include “Documentation of authorization for cyber security patch implementation.” Calling out cyber security patches under this measure of authorization outside of a “change request record” as opposed to applying it to the other items may cause confusion regarding differing expectations for cyber security patches. This statement should be more generalized for the other CIP-010 R1.1 items as well.

Agree with change to CIP-010. Do not agree with Glossary of Terms

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI supports many of the proposed NERC Glossary terms, however, concerns remain with those terms identified in our comments above. EEI also notes that the phrase “SCI identified independently” is unclear in its intent and needs to be clarified before EEI can support the revisions to CIP-010. For this and the following concerns we cannot support the proposed changes at this time

1) Subpart 1.2.2 could be interpreted to allow mixed trust. The language does not provide sufficient clarity to ensure mixed trust is not allowed.

2) There is a typo in the Applicable Systems part of Requirement 2, Part 2.1, Table R2. SCI is incorrectly identified as CI.

3) Attachment 1 – Section 3; Removable Media; Part 3.2: the removal of language identifying high impact or medium impact BES Cyber Systems appears to expand this obligation beyond its original intent. EEI recommends that the original language be restored.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers these additional comments:

- ERCOT appreciates the removal of part 1.1.5 from the requirement language since patches would be covered under parts 1.1.1 and 1.1.2. However, the measure should be updated to be consistent with the requirement language.

- For Part 3.3, the requirement to build outside of the production environment and perform the vulnerability scan has been removed.

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 agrees with the overall concepts but has several specific issues with the language.

In R1.1.1 the last "or firmware;" seems to be in error as firmware has already been covered in the list. The measures for this requirement could also use examples of evidence in regards to parent/child images such as VDI.

In R1.1.3 'including-applications containers' should be 'including application containers'

In R1.1.4 by including SCI in applicability, is the intent to know and authorize change to the SCI underlay communications at the IP port level? Typically the SCI underlay is service level due to the proprietary nature of the communication protocols, but 1.1.4 only allows services if one is unable to determine ports. Since you can always determine port numbers in use, this requires authorizing changes to port numbers within the underlay and not services, which may not be possible or of no value.

Also R1.1.4 could be improved by clarifying that the authorization is for a change to the OS, software, or configuration that subsequently will change ports or port ranges. Port numbers may be dynamically changing in real-time during process execution and further clarity around the level of change authorization intended is needed. As currently worded, a change authorization could be required every time a logical port is opened or closed by an executing process.

In R3.3, it would be clearer to state "Perform an active vulnerability assessment of a new Applicable System prior to it becoming a new Applicable System…" We suggest it helps with clarity to lead with the main required action and then follow it with the timing aspect of the 'prior to' phrasing rather than leading with it.

In R4, the scoping is set to “not lows”, which includes everything outside of CIP scope. The scoping has been removed from Attachment 1 as well, leaving the scoping for this requirement within the glossary definitions of TCA and RM. While this works, we’d prefer the scoping to be in the requirements within the standard.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	No

Document Name	

Comment

AWS agrees with changes to CIP-010 R1, R2, and R3. CIP-010 R4 has been updated to accommodate Virtual Cyber Assets and virtual machines hosted on physical Transient Cyber Assets, but because the standard language allows a Responsible Entity to choose one or a combination of security controls there may be security control gaps.

Since the TCA definition explicitly states that a VM running on a physical TCA can be treated as software running on the physical TCA, the VMs could be vulnerable to security threats undetected by the physical host. The Standard does not require additional security controls to be applied to the VMs running on physical TCAs.

We propose removing the language “Virtual machines hosted on a physical TCA can be treated as software on that physical TCA” from the TCA definition, and modifying the VCA definition to read, “A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure, a PCA, or a TCA.”

Likes 0	
Dislikes 0	

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer	No
Document Name	

Comment

<duplicate>

Likes 0	
Dislikes 0	

Response

Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1

Answer	No
Document Name	

Comment

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Likes 0	
Dislikes 0	

Response

David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan

Answer	No
Document Name	

Comment

OPG concurs with NPCC's RSC comments

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- The complete removal of the term “baseline” creates a gap for the change management of Cyber Systems, similar to the removal of “ESP” that was re-instated. Recommend in CIP-010 R1 P1.1 allow for the continuation of “Baselines” at least in the measure as an option if not within the standard language.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We disagree with the changes in CIP-010.

Recommendations:

- For CIP-010 R1.1, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-010 R1.2, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA.
- For CIP-010 R1.3, R1.4 and R1.5, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-010 R2, R3, R4 and their Parts, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

See what SRP stated in Question 2 and 11. Needs more clarity.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

In support of IRC SRC/SWG.

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Likes 0	
Dislikes 0	
Response	

Michael Brytowski - Great River Energy - 3	
Answer	No
Document Name	
Comment	

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE requests greater clarification regarding the phrase in CIP-010-5 R3.3 "Prior to becoming a new Applicable System...". Does this mean when a Cyber Asset receives categorization per CIP-002 or some later phase of the deployment lifecycle? Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System” Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching? We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable. Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation. Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope? Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration? Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions	

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Requirements 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above, SDT should be more precise. Requirement 1.1.5 (.1.5. Any security patches applied.) was removed, yet the measure “Documentation of authorization for cybersecurity patches implementation” was added as evidence of change authorization for security patches. Need for clarification as the change seems contradictory.

We suggest that the SDT review the wording of requirement 1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware; This requirement mention ‘’images’’, why not use the word ‘’container’’?

Requirement 1.2 The overall requirement is questionable. Enforcing restrictions on the sharing of CPU or memory between systems limits the possible gain of instating virtualization. Also following the new definition of ESP, the latter is enforced by an EACMS and not by the SCI. We suggest that the SDT reviews their objectives and how to implement them.

Requirement 1.3 To be coherent shouldn't this requirement refer also to 1.2. After all, the CPU and memory controls are CIP-007 and the ESP is CIP-005. Follow the same logic as 1.4, i.e. ‘’for each change to the items listed in Part 1.1 or Part 1.2’’.

Requirement 1.4 no comments

Requirement 1.5 Our understanding is that we don’t need to verify the source nor the integrity of the security patches any longer. Since CIP-007 Patch management does not include those checks, wouldn’t this be considered as neglecting a compliance sound practice? (To validate the security patches)? Is this the real intent of the SDT?

Requirement 2.1 no comments

Requirement 3.3 What does ‘’Prior to becoming a new Applicable System” means?

We suggest that the SDT defines ‘’becoming’’. Is the intent of the SDT to permit the creation of a virtual cyber asset on an SCI, this SCI being in a production environment? We suggest that the SDT review the usage of ‘’production environment’’ versus ‘’becoming’’.

There is a need for additional clarification for “same type” in “like replacements of the same type of Cyber System”. Is ‘’type’’ associated with the Cyber System definition?

Since the baseline configuration doesn’t exist anymore, what is the intent of the SDT with the usage of the word ‘’configuration’’? How does one entity define configuration?

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments 1:

We disagree with the changes in CIP-010.

Recommendations:

· For CIP-010 R1.1, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

· For CIP-010 R1.2, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA.

· For CIP-010 R1.3, R1.4 and R1.5, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

· For CIP-010 R2, R3, R4 and their Parts, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	

Comment

· R1.1 – application containers is not a well-defined term and should be clarified if it is going to be used in the Standards.

· R1.1 - The addition of “Documentation of authorization for cyber security patch implementation” into the Measures does not align with the removal of “Security patches applied” from the requirements of Part 1.1

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Requirements 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above, SDT should be more precise. Requirement 1.1.5 (.1.5. Any security patches applied.) was removed, yet the measure “Documentation of authorization for cybersecurity patches implementation” was added as evidence of change authorization for security patches. Need for clarification as the change seems contradictory.

We suggest that the SDT review the wording of requirement 1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware; This requirement mention ‘’images’’, why not use the word ‘’container’’?

Requirement 1.2 The overall requirement is questionable. Enforcing restrictions on the sharing of CPU or memory between systems limits the possible gain of instating virtualization. Also following the new definition of ESP, the latter is enforced by an EACMS and not by the SCI. We suggest that the SDT reviews their objectives and how to implement them.

Requirement 1.3 To be coherent shouldn't this requirement refer also to 1.2. After all, the CPU and memory controls are CIP-007 and the ESP is CIP-005. Follow the same logic as 1.4, i.e. ‘’for each change to the items listed in Part 1.1 or Part 1.2’’.

Requirement 1.4 no comments

Requirement 1.5 Our understanding is that we don’t need to verify the source nor the integrity of the security patches any longer. Since CIP-007 Patch management does not include those checks, wouldn’t this be considered as neglecting a compliance sound practice? (To validate the security patches)? Is this the real intent of the SDT?

Requirement 2.1 no comments

Requirement 3.3 What does ‘’Prior to becoming a new Applicable System” means?

We suggest that the SDT defines ‘’becoming’’. Is the intent of the SDT to permit the creation of a virtual cyber asset on an SCI, this SCI being in a production environment? We suggest that the SDT review the usage of ‘’production environment’’ versus ‘’becoming’’.

There is a need for additional clarification for “same type” in “like replacements of the same type of Cyber System”. Is ‘’type’’ associated with the Cyber System definition?

Since the baseline configuration doesn’t exist anymore, what is the intent of the SDT with the usage of the word ‘’configuration’’? How does one entity define configuration?

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

R1-Removing baseline configuration does not change what needs to be done in practice. Entities will still need to retain a baseline configuration as evidence from which to establish the changes that were authorized.

- For Part 1.4 an entity will still need to show the baseline configuration prior to the change to show required cyber security controls in CIP-005 and CIP-007 are not adversely affected.

- For Part 2.1 an entity will still need to provide baseline configurations for evidence that they monitor at least once every 35 calendar days for unauthorized changes to the items listed Parts 1.1 and 1.2.

R3- The concern is that Remediation VLANs should be properly defined in the technical rational or Glossary as it may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.

Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	

We support NPCC TFIST's comments as found below:

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Per CIP-010 R1, Part 1.1, the requirement to authorize all changes is very broad in terms of reference to OS, software applications, logical network accessible ports, etc. Per the strict language of the proposed standard, it is not clear what constitutes a change. Does the modification of a desktop background constitute an OS change? While it is expected the SDT intended to limit the nature of changes to versions or upgrades of OS and software and patches for example, the chosen language leaves this open to interpretation. BC Hydro recommends adding more clarity here with the language of the standard. The Technical Rationale is not used as actual compliance guidance as indicated by NERC and without explicit language in the standard or without an endorsed compliance guidance document to supplement, the SDT's intent will be subject to the interpretation of audit entities. Also, it is not clear if these changes to be authorized are restricted only to changes to pre-existing CIP Systems or as part of the commissioning of a new CIP System. While the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the SCI definition proposed in this project comment/ballot submission. Attachment 1 to CIP-010 covering TCA and RM requirements have removed any context of what RM is expected to be connected to. It is not clear if the SDT intended for this removal to imply connection to any CIP System or to any non-CIP System? Recommend restoring the deleted text which referenced high and medium impact BES Cyber Systems, PCAs, and associated networks but to also include applicable SCIs, etc.to provide context.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	

The last proposed draft by this SDT of the Standards, though it used far more new definitions, seemed clearer. It's not clear what the existing changes are solving, nor is it clear what part(s) of the glossary of terms this question is addressing.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA does not support the modified language in CIP-010. How SCI is to be independently identified is not clear.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)

Answer	No
Document Name	

Comment

Comments:

R1.1:

Could the SDT explain why the security patches were removed?

What measures are in place to include alternate changes?

R1.2:

Is the SDT not including non CIP Assests to bring in all assets into the program by default?

Definitions:

Recommend the SDT provide an interpretation of the definition for Self-Contained Application. As written, the definition seems confusing, and could have the potential to be misinterpreted.

Recommend the SDT define and provide an interpretation in the scope of what it means by “Authorized Changes”.

R1.4 and R1.5:

Is the SDT asking for entities to include both firmware and OS? In the past, entities could not show firmware if an OS was present. This has the potential to broaden the scope, and includes authorized changes to the OS. Any changes to the OS would be included in scope and would have to be tested as part of 1.4 and 1.5. In the past, if the baseline was not changed, then the entity would not have concern about R1.4 and 1.5. This new standard will change that, and potentially add additional work for entities when a change is made. This could open entities to an investment in new tools because baseline is being removed.

R2.1:

Recommend defining in each subpart what is the change.

These changes seem broader than virtualization, is this in line with scope of the SAR?

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Several of the terms and their usage, especially SCI, lends ambiguity with their use in the revised CIP-010 Standard. Further clarifications and refinements of the terms should be given attention.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	

Comment

The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. Additionally, question #12 begins by asking about the revised CIP-010 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-010.

We are concerned about revising the existing CIP standards to address virtual technologies. We recommend any necessary requirements pertaining to change management of virtual cyber assets used for a CIP function be encoded in a new Reliability Standard. Please see our comment on this in response to question #14.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
In R1.1.1, need for clarification as to the meaning of "…images used to derive operating systems". In Measures of R1.1, "Documentation of authorization for cyber security patches implementation" was added as evidence of change authorization for security patches, but the requirement for authorize change to security patches (formerly 1.1.5) was removed. Need for clarification as the change seems contradictory. In R1.5, need for clarification as to why prior to a change associated with security patches (formerly 1.1.5) was removed. In R1.3, since changes to SCI Configuration mentioned in R1.2 may impact CIP-005 controls, R1.2 should also be included similarly to R1.4 "For each change to the items listed in Part 1.1 or Part 1.2". In R3.3, need for clarification for "same type" in "…like replacements of the same type of Cyber System…"	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS agrees with EEI's comments on the repeated use of the undefined term "application container" causing confusion, as well as Attachment 1 – Section 3; Removable Media; Part 3.2: the removal of language identifying high impact or medium impact BES Cyber Systems appears to expand this obligation beyond its original intent. AZPS recommends that the original language be restored.	
Likes 0	

Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
See response to question 6 and 8.	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
We support the changes to the Requirements and Measures of R3.3. The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy generally agrees with the approach enumerated by the SDT but notes that the inclusion of “application containers” must be addressed in the Technical Rationale document if it remains an undefined term. There is currently no explanation for this inclusion, leaving RE’s subject to auditor interpretation. Additionally, subpart 1.2.2 seems unnecessarily constrained and should likely include all changes to configuration that enforces an ESP.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy does not agree with the proposed changes in CIP-010. Independly identified SCI is listed throughout the applicable systems column and with our concern with the lack of clarity in Independly identified SCI, we can not support at this time. While Xcel Energy does not support the approval of this Standard at this time, we do support other aspects in the modifications made as identified in EEI comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
There is insufficient clarity to ensure consistent outcomes in monitoring security controls.	
Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	

Comment
No. Please see NRG's response to question 2 for additional detail.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	

Comment
No. Please see NRG's response to question 2 for additional detail

Likes 0	
Dislikes 0	

Response

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

Comment
CIP-010 R3.3 – Reclamation recommends adjusting the language. From: "Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for:". To: "Prior to the Entity commissioning a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for:".

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
ACES agrees with the proposed changes to CIP-010 as long as “SCI identified independently…” is clarified based on question #2.	
Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC recommends that CIP-010 be reviewed to ensure consistent usage of he acronym "BCS" versus BES Cyber System. Additionally, the proposed language in CIP-010 R 1.1.2 to include and address 'application containers' is confusing and unlikely to lead to the expected protections. Neither CIP-010 nor the proposed definitions address the definition of or criteria determinative of an "application container." Additionally, the technical rationale also does not address what such 'application containers' consist of or provide language or criteria defining them. Accordingly, GSOC recommends providing additional defining language around the nature and scope of such 'application containers.'	
Likes 0	
Dislikes 0	
Response	

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

Tacoma Power supports the proposed language, and has the following recommended edits:

- For CIP-010 R1.2, change language in the Applicable Systems column to match the Applicable Systems language used in CIP-007 R1.3
- Consider using a clearer or more commonly referenced word other than "instantiation" in CIP-010 R3.4 measures
- Correct typo in the second bullet in CIP-010 R3.4 measures: "Documention" should be "Documentation"
- For CIP-010 Attachment 1, Section 1.3 and 1.4, re-word the second bullet to state "Controls that maintain the last known good state of..."
- For CIP-010 Attachment 1, Section 2.2, re-word the fourth bullet to state "Review of controls that maintain the last known good state of..."
- Remove the ";" at the end of R1 Part 1.1.1 "; or firmware;" The reference here is back to the disk image used to derive, not stand alone firmware. So 1.1.1 should read: "1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems or firmware;"

Likes 0	
Dislikes 0	
Response	

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	

Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

AEP supports the changes but has identified the following concerns:

The repeated use of the undefined term “application container” could cause confusion. Given this term is an important part of CIP-007 Requirements, it should be defined.
AEP does not support the need for the note in requirement 1.5 under Applicable Systems. We were not able to rationalize the note in Requirement 1.5 to contracts and thereby suggest removal of this note.
There is a typo in the Applicable Systems part of Requirement 2, Part 2.1, Table R2. SCI is incorrectly identified as CI.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	Yes
Document Name	

Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE agrees with the proposed definition for TCA.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	

CEHE agrees with the proposed definition for TCA.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	Yes
Document Name	

Comment

ACES agrees with the proposed changes to CIP-010 as long as “SCI identified independently…” is clarified based on question #2.

AEPC signed on to ACES comments.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	Yes
Document Name	

Comment

We support these approach used for these changes once acceptable definitions are in place.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	

Comment
Part 1.3, should ‘applications containers’ be changed to ‘application containers?’ Part 1.1.4, suggest changing language to be consistent with CIP-007-7, Part 1.1 – Any network accessible Internet Protocol (IP) ports (or services if unable to determine ports). Part 1.2.1, would it better scope the ‘system’ was changed to CIP Systems. Controls sharing of CPU or memory between (systems)DELETE (CIP Systems)ADD with different impact ratings, including non-CIP Systems, hosted on SCI; and Part 3.3, first bullet – would it be more accurately scoped to change ‘Cyber System’ to CIP System? like replacements of the same type of CIP System with a configuration of the previous or other existing CIP System; or

Likes 0	
Dislikes 0	

Response

Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	

Comment
We agree with the proposed changes to CIP-010. Does CIP-010 R1.3 intentionally not apply to changes made to items listed in Part 1.2?

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	

Comment
Chelan approves of the changes to CIP-010.

Likes 0	
Dislikes 0	

Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE noticed that proposed CIP-010 R4 language references the definitions of Transient Cyber Assets (TCA) and Removeable Media to define in scope devices for the requirement R4. For purposes of clarity, Texas RE recommends revising the requirement language to indicate which devices are in scope within the requirement language itself. Texas RE proposes the following language:

Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented processes that include each of the applicable requirement parts in Table CIP-010-x Table R4:

Applicable Systems

High Impact BCS and their associated:

1. SCI; and

2. PCA

Medium Impact BCS and their associated:

1. SCI; and

2. PCA

Requirement 4 Part 1

One or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1, except for use on low impact BCS or SCI supporting only low impact BCS(s).

Additionally, Texas RE continues to be concerned that security obligations will be reduced by removing the reference to baseline configurations. Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 5), CM-2 Baseline Configuration, which states, "*Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-*

upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture."

Likes 0	
Dislikes 0	

Response

13. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

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

Answer	No
Document Name	

Comment

Please refer to Dominion Energy's response Q14C below regarding CIP-004 and ERC as well as our comments to Q1.

There appears to be ambiguity on whether this pull in EACMS devices because of SCI? Clarity is needed.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

No. Please see NRG's response to question 2 for additional detail.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

No. Please see NRG's response to question 2 for additional detail.

Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Conforming changes to CIP-003 - CIP-013 are dependent on ambiguous definitions introduced in CIP-002 and CIP-005.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy generally supports conforming changes to these standards. However, Xcel Energy does not agree with the proposed changes to the applicable systems column in these standards. Independly identified SCI is listed throughout the applicable systems column and with our concern with the lack of clarity in Independly identified SCI, we can not support at this time. While Xcel Energy does not support the approval of this Standard at this time, we do support other aspects in the modifications made as identified in EEI comments.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	

Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	

Comment
We do not agree with the proposed changes to these Reliability Standards and do not believe these specific standards need revising. The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards. Second, the proposed change is only to include the phrase “SCI identified independently supporting an Applicable System.” As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase. If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include “Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.” This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.] We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	

Comment
Comments: Comments: For the CIP-013 Standard, we do not agree with the part 4.2.3 Exemptions, specially 4.2.3.3. How do you define “Cyber systems who provide confidentiality and integrity of an ESP that extends to one or more geographic locations” ?

Suggestion: 4.2.3.2 Cyber Systems *and Shared Cyber Infrastructure(SCI)* associated with communication links logically isolated from, providing *or not* logical isolation between discrete Electronic Security Perimeters (ESP).

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	

Comment

We do not agree with the proposed changes to these Reliability Standards and do not believe these specific standards need revising.

The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards.

Second, the proposed change is only to include the phrase “SCI identified independently supporting an Applicable System.” As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase.

If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include “Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.” This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.]

We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Several of the terms and their usage, especially SCI, lends ambiguity with their use in the Standards. Further clarifications and refinements of the terms should be given attention.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CIP-003: In requirement R2 refers to “SCI that supports any part of a low impact BCS” but the VSL for R2 only refers to “SCI” without stating “that supports any part of a low impact BCS.”

CIP-004: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-006: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-008: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-009: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-011: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-013: CEHE proposes to replace “SCI identified independently supporting these BCS or their associated EACMS and PACS.” with “independent SCI that supports these BCS or their associated EACMS and PACS.” In the VSLs for R1 and R2 it refers to “… BES Cyber Systems, and their associated EACMS, PACS, and SCI, …”, there are no descriptors around SCI, such as “independent SCI”.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment
NCPA does not support the modified language. How SCI is to be independently identified is not clear.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment
CIP-003: In requirement R2 refers to “SCI that supports any part of a low impact BCS” but the VSL for R2 only refers to “SCI” without stating “that supports any part of a low impact BCS.” **CIP-004:** SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.” **CIP-006:** SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.” **CIP-008:** SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.” **CIP-009:** SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.” **CIP-011:** SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.” **CIP-013:** SIGE proposes to replace “SCI identified independently supporting these BCS or their associated EACMS and PACS.” with “independent SCI that supports these BCS or their associated EACMS and PACS.” In the VSLs for R1 and R2 it refers to “… BES Cyber Systems, and their associated EACMS, PACS, and SCI, …”, there are no descriptors around SCI, such as “independent SCI”.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No

Document Name	
Comment	
The last draft of the standard seemed clearer. It's not clear what the existing changes are solving.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
All of the standards (CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013) referred in this question are proposed with a change the phrase "SCI identified independently supporting an Applicable System." This phrase requires more clarity from the SDT team as to what is meant by an SCI being independent and as well as supporting an applicable system. The terms used here have some level of ambiguity specifically when used in conjunction with each other. SDT is requested to provide examples and better clarity on this phrase as it pertains and becomes applicable as a proposed change to all of the above listed standards. Secondly as advised in the comments above while the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the SCI definition proposed in this project comment/ballot submission. As explained in the comments of Questions 10 related to CIP-005, Question 11 related to CIP-007 and Question 11 related to CIP-010 above BC Hydro does not agree with the changes in the NERC glossary of terms introduced in Draft 2 of Project 2016-02.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs For CIP-011, see BCSI comment in Q8	

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – "EERC"

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	

Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – "EERC"

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

It is difficult to agree with the revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 standards as there are too many questions and uncertainty surrounding the proposed changes.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

While AEP supports conforming formatting changes and removal of Background and Technical Rationale, we do still have concerns regarding some of the terms proposed to be added to Applicable Systems (as stated in the responses to Questions #1 through #8 above). We recommends adding clarification on “SCI identified independently”, as this phrase has been added to Applicable Systems column for many of the CIP standards. AEP recommends that the terms and definitions should be clarified before included in the standard revisions.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments 1:

We disagree with the changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.

Recommendations:

· Resulting from our proposed changes to the definitions (See our comments in Q1), we suggest removing SCI language from all Applicable Systems.

Comments 2:

We do not agree with the proposed changes to these Reliability Standards and do not believe these specific standards need revising.

The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply

regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards.

Second, the proposed change is only to include the phrase “SCI identified independently supporting an Applicable System.” As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase.

If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include “Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.” This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.]

We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013’s use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – “EERC”

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

It is difficult to agree with the revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 standards as there are too many questions and uncertainty surrounding the proposed changes.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment
GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	

Comment
In support of IRC SRC/SWG. For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs For CIP-011, see BCSI comment in Q8 Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2. Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013? Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version. Request correction of typo in CIP-006 R2.2 Applicability – "EERC" Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

The proposed changes to the above requirements (CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013), should not be revised, but be left as is.

Since these requirements are policy and process focused than the technical requirements of CIP-005, CIP-007 and CIP-010. In saying this (CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013) should apply regardless of technology.

Again the phrase “SCI identified independently supporting an Applicable System” The phrase is confusing and up to interparation.

We do not agree with the proposed changes to these Reliability Standards and do not believe these specific standards need revising.

The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards.

Second, the proposed change is only to include the phrase “SCI identified independently supporting an Applicable System.” As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase.

If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include “Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.” This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.]

We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	

Comment

We do not support the proposed changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.

Recommendations:

- Resulting from our proposed changes to the definitions (See our comments in Q1), we suggest removing SCI language from all Applicable Systems.

The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards.

Second, the proposed change is only to include the phrase “SCI identified independently supporting an Applicable System.” As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase.

If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include “Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.” This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.]

We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3

Answer	No
Document Name	

Comment

CIP-003 Requirement 2/Attachment 1 appear to either be in conflict or redundant to CIP-010 R4 where the language “except for use on low impact BCS or SCI supporting only low impact BCS(s)”. The actual requirements for TCA for Low BCS are ambiguous given this redundancy or conflict.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	
For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs	

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – "EERC"

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

Likes 0	
Dislikes 0	

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer	No
Document Name	

Comment

<duplicate>

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments.

Likes 0	

Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI supports the changes made to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011 and CIP-013 except as described below:

- CIP-003: EEI supports the proposed conforming changes but proposes the following for Attachment 1 Section 5, 5.1 and 5.2.

  "Controls that maintain the state of the operating system and software such that it is in a known state prior to use;".

- CIP-004: The phrase "SCI identified independently" is frequently used throughout CIP-004 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard.
- CIP-006: The phrase "SCI identified independently" is frequently used throughout CIP-006 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard. The following concerns should also be addressed:

1) *Requirement R1, Subpart R1.10 was removed and the technical rationale states that the requirements were fully moved to CIP-005, Subpart 1.4 but their associated PCAs were not included, which represents an unintentional reliability gap.*

2) EEI notes that within the Applicable Systems column of Part 1.1, the term "hosting" is used in "SCI without ERC hosting Medium Impact BCS", but "hosting" has been changed to "supporting" in other places.

- CIP-008: The phrase "SCI identified independently" is frequently used throughout CIP-008 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard.
- CIP-009: The phrase "SCI identified independently" is unclear. Additionally, restoration plans as currently described are too prescriptive and should not be tied to the restoration of SCI even if an entity intends to utilize virtualization. The focus should be the restoration of critical systems necessary for restoration and not predefine how entities define their restoration plans. For example, an entity may decide to incorporate into their restoration plan a more barebones approach that restores an image to a dedicated server without the restoration of SCI. While this may not restore their systems in an identical fashion to what they were operating prior to the failure, it would allow them to quickly and efficiently restore their critical systems. The objective of a recovery plan should focus on the recovery of those critical systems (i.e., BCS, EACMS and PACS functionality). For those entities who chose to take another approach such as restore their SCI as a part of their recovery plan, they too would not be limited by this Reliability Standard. Such an approach would provide flexibility and promote a results-based approach.

Applicable Systems column of Parts 2.1 and 2.2, the term "hosting" is used in "SCI hosting Medium Impact BCS at Control Centers or their …", but "hosting" has been changed to "supporting" in other places. This difference should either be explained or corrected if it was an unintentional error.

- CIP-011: The phrase "SCI identified independently" is used throughout CIP-011 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard. .
- CIP-013: The phrase "SCI identified independently" is used in Requirement R1 of CIP-013 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard.

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	

Comment

For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – "EERC"

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

It is difficult to agree with the revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 standards as there are too many questions and uncertainty surrounding the proposed changes.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – "EERC"

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Nurul Abser - NB Power Corporation - 1

Answer	No
Document Name	

Comment

With respect to CIP-011 changes, R.1.2. and R.2.1. appear to be the same requirement. We suggest incorporating the measure for R2.1 into R1.2 and eliminating R.2.1.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Chelan agrees with the conforming changes.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
CIP-003: Section 3.1 - suggest removing ‘as determined by the Responsible Entity’ as it is already stated in Attachment 1. Section 3.1, second bullet – Change ‘an SCI’ to just SCI Section 3.1, Should ‘and a system(s) outside:’ be changed to ‘and a Cyber System outside:’ CIP-004, Part 2.1.9 – Would the intended scope be more accurate by changing Cyber Systems to CIP Systems? Cyber security risks associated with electronic interconnectivity and interoperability with other CIP Systems, including Transient Cyber Assets, and with Removable Media. CIP-013, R1.1 and R1.2 – Would the scope more accurately be identified by changing ‘system’ to ‘CIP Systems?’	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	

AZPS agrees with the proposed conforming changes to the Reliability Standards, *except* for the following:

CIP-006 R1.10 is not fully covered by CIP-005 R1.4 as it leaves the associated PCAs unaccounted for.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	Yes
Document Name	

Comment

ACES supports the changes and does not believe the inclusion of “SCI identified independently…” in these standards increase compliance burden and are used for clarification of what is included in the Applicable Systems. Our opinion is predicated on clarifying “SCI identified independently…” as noted in question #2.

AEPC signed on to ACES comments.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	Yes
Document Name	

Comment

SDG&E supports EEI Comments

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	Yes
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
We agree with the conforming changes. However, please correct the CIP-003 exemption to be consistent with the other standards.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	

Answer	Yes
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
We agree with the confroming changes. However, please correct the CIP-003 exemption to be consistent with the other standards.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Tacoma Power agrees with the proposed changes to the NERC Glossary terms. However, we identified the following improvements and minor corrections to the CIP-003 and CIP-006 documentation: • CIP-003 Attachment 1 Section 1 has inconsistent language for the inclusion of SCI. Suggest modifying to “...SCI that supports any part of a low impact BCS...” • CIP-009 R2.1 and R2.2, the redline should delete the following item from the Applicable System column: “SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS”	
Likes 0	
Dislikes 0	
Response	

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	
Comment	
We agree with the conforming changes. However, please correct the CIP-003 exemption to be consistent with the other standards.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Relative to CIP-003, the inclusion of a reference to SCI in R2, which addresses low impact assets, would seem to suport the inclusion of SCI where SCI is independently identified, but supporting a high or medium impact BCS. However, this language was struck from the requirement despite the fact that independently identified BCS supporting an applicable system is subject to several requirements and standards addressed within the policies required under R1. Further, this raises a question as to whether SCI grouped with BCS would be subject to CIP-003 by virtue of their grouping while independently identified SCI would not. For this reason, GSOC requests clarification regarding whether SCI that is identified independent of BCS, but is supporting such systems should be addressed in the policies required under CIP-003, R1. **Relative to CIP-005, GSOC recommends revising the following language** **Real-time Assessment and Realtime monitoring data while being transmitted between Control Centers subject to CIP012; and** **as follows:** **Real-time Assessment and Realtime monitoring data subject to CIP012; and.**	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes

Document Name	
Comment	
ACES supports the changes and does not believe the inclusion of “SCI identified independently…” in these standards increase compliance burden and are used for clarification of what is included in the Applicable Systems. Our opinion is predicated on clarifying “SCI identified independently…” as noted in question #2.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
No comments	
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	
For CIP-006 R1.1, Southern believes the first "SCI without ERC hosting Medium Impact BCS" is unnecessary and we suggest deletion. For CIP-009, we suggest deleting "SCI identified independently" throughout the standard. The goal of CIP-009 according to R1.3 and the GTB is to recover the functionality of the BCS. In the "all-in" scenario, the SCI underlay isn't called out as a specific component of a recovery plan. To recover the functionality of a system, such as a virtualized EACMS, the entity may restore an image to a dedicated server HW without SCI. The SCI should not be a specific object of recovery plans - the object is to recover the BCS, EACMS, or PACS functionality. If recovery of the SCI is required by the entity to recover the BCS functionality, that would be required as part of the plan but not a distinct object of the requirement. If SCI applicability is left in CIP-009, it seems duplicated throughout most of R2's requirement parts. The edits made in R1 and R3 to applicable systems were not made in R2. The 'applicable system' in R2.2 should be capitalized. R2.2 and in particular its measures need to be updated for virtualization scenarios. It maintains a sense of tape backups of static files.	
Likes 0	

Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
We agree with the conforming changes. However, please correct the CIP-003 exemption to be consistent with the other standards.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
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	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

14. Please provide any additional comments for the SAR drafting team to consider, if desired.

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	
Document Name	

Comment

Portland General Electric Company is providing the following comments for the drafting team's consideration:

CIP-005-8 R2.6.2 – “Applicable Systerms” is used instead of “Applicable Systems”

CIP-005-8 R2.1 - In the Applicable Systems column, the phrase "Intermediate Systems used to access Applicable Systems of Part 2.1" is included. However, the requirement states that Responsible Entities must "Permit authorized IRA, if any, only through an Intermediate System." Portland General Electric Company believes this implies that an Intermediate System would need to broker access to the Intermediate System that is brokering access to the other Applicable Systems in R2.1. Portland General Electric Company wonders if it was the drafting team’s intent to include "Intermediate Systems used to access Applicable Systems of Part 2.1."

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	
Document Name	

Comment

Portland General Electric Company is providing the following comments for the drafting team's consideration:

CIP-005-8 R2.6.2 – “Applicable Systerms” is used instead of “Applicable Systems”

CIP-005-8 R2.1 - In the Applicable Systems column, the phrase "Intermediate Systems used to access Applicable Systems of Part 2.1" is included. However, the requirement states that Responsible Entities must "Permit authorized IRA, if any, only through an Intermediate System." Portland General Electric Company believes this implies that an Intermediate System would need to broker access to the Intermediate System that is brokering access to the other Applicable Systems in R2.1. Portland General Electric Company wonders if it was the drafting team’s intent to include "Intermediate Systems used to access Applicable Systems of Part 2.1."

CIP-006-7 R1.6 - In the Applicable Systems column, there should be a bullet next to "Medium Impact BCS with ERC" so that the Applicable Systems column reads "Physical Access Control Systems (PACS) associated with: • High Impact BCS, or • Medium Impact BCS with ERC"

CIP-006-7 R1.6 - The requirement language says, "Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System." However, SCI identified independently is only supporting PACS, not categorized as part of the PACS itself. For clarity, Portland General Electric Company suggest rephrasing the requirement language to say, "Monitor Applicable Systems for unauthorized physical access."

CIP-006-7 R1.7 - The requirement language says, "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection." However, SCI identified independently is only supporting PACS, not categorized as part of the PACS itself. For clarity, Portland General Electric Company suggest rephrasing the requirement language to say, "Issue an alarm or alert in response to detected unauthorized physical access to an Applicable System to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection."

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	
Document Name	

Comment

Overall, the ISO/RTO Council (IRC) Standards Review Committee (SRC)[1] recommends a separate virtualization standard be adopted to reduce the amount of change, additional work and confusion that will be required by a more holistic change as noted by the SDT. The new standard should be limited to only the requirements that directly relate to virtualization technology (e.g. dedicated infrastructure, shared infrastructure and management systems). In the event the SDT declines to pursue a separate virtualization standard, the SRC offers these comments in Questions 1-14 on the draft standards as presented.

Are these comments for the SAR drafting team or the Standards drafting team per the question’s text?

Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries.

Request that the SDT post the draft revisions as “red-line to last approved” rather than “to last posted.” This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates.

Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, SPP and PJM (with the exception of our response to question 14, paragraph 1).

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

N&ST believes the proposed “Exemption” statement in every CIP Standard, 4.2.3.3, “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an Electronic Security Perimeter (ESP) that extends to one or more geographic locations” is both confusing and inaccurate. One provides for the confidentiality and integrity of data, not ESPs. N&ST suggests rewording that’s consistent with the language of proposed CIP-005 Requirement R1 Part 1.4, such as “Cyber Systems associated with communication links used to span a single ESP among two or more geographic locations.”

N&ST reviewed proposed VSL revisions only briefly, but noticed the High and Severe VSLs for CIP-005 Requirement R1 still refer to Requirement Parts (1.2.1 through 1.2.3) that the SDT has deleted. N&ST recommends a thorough proofreading of all VSLs to ensure they reflect the latest proposed Requirement changes.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	
Document Name	

Comment

Portland General Electric Company is providing the following comments for the drafting team's consideration:

CIP-005-8 R2.6.2 – “Applicable Syste[r]ms” is used instead of “Applicable Systems”

CIP-005-8 R2.1 - In the Applicable Systems column, the phrase "Intermediate Systems used to access Applicable Systems of Part 2.1" is included. However, the requirement states that Responsible Entities must "Permit authorized IRA, if any, only through an Intermediate System." Portland General Electric Company believes this implies that an Intermediate System would need to broker access to the Intermediate System that is brokering access to

the other Applicable Systems in R2.1. Portland General Electric Company wonders if it was the drafting team's intent to include "Intermediate Systems used to access Applicable Systems of Part 2.1."

CIP-006-7 R1.6 - In the Applicable Systems column, there should be a bullet next to "Medium Impact BCS with ERC" so that the Applicable Systems column reads "Physical Access Control Systems (PACS) associated with: • High Impact BCS, or • Medium Impact BCS with ERC"

CIP-006-7 R1.6 - The requirement language says, "Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System." However, SCI identified independently is only supporting PACS, not categorized as part of the PACS itself. For clarity, Portland General Electric Company suggest rephrasing the requirement language to say, "Monitor Applicable Systems for unauthorized physical access."

CIP-006-7 R1.7 - The requirement language says, "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection." However, SCI identified independently is only supporting PACS, not categorized as part of the PACS itself. For clarity, Portland General Electric Company suggest rephrasing the requirement language to say, "Issue an alarm or alert in response to detected unauthorized physical access to an Applicable System to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection."

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Are these comments for the SAR drafting team or the Standards drafting team per the question's text?

Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries

Request that the SDT post the draft revisions as "red-line to last approved" rather than "to last posted." This expectation is consistent with the posting of other NERC Standards and earlier postings of CIP updates.

Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	
Document Name	
Comment	

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0	
Dislikes 0	
Response	

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	
Document Name	
Comment	

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	
Document Name	
Comment	

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0	
Dislikes 0	
Response	

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	
Document Name	
Comment	

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	

Planned and Unplanned changes language should be added to the Implementation Plan, similar to the language included in previous CIP implementation plans. *(See Implementation Plan For Version 5 CIP Cyber Security Standards, November 7, 2011; Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012; and Implementation Plan - Project 2014-02 CIP Version 5 Revisions, January 23, 2015.)*

Likes 0	
Dislikes 0	
Response	

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	
Document Name	
Comment	

PJM appreciates and supports the continued work of the Standards Drafting Team (SDT) to transition the framework of the NERC CIP standards to one that more readily supports the use of virtualization technology. While PJM recognizes the significant challenges associated with developing revisions and building consensus within the industry, we believe it is critical to sustain the current momentum and finalize these changes. These changes are important not only to better enable the use of virtualization technology to support the reliability of BES Cyber Systems, but also – and more importantly - to better enable the industry’s use of emerging technologies in the future. PJM believes the SDT’s work to update the standards framework will position the industry to take earlier advantage of new technologies to increase reliability as the revised standards will be based more on controls rather than

technology type. While there is the possibility that changes to the standards could still result from the introduction of new technologies, these changes should be minimal if the framework of the standards is based on controls.

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	
Document Name	

Comment

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

1) Planned and Unplanned changes language is missing in this version’s implementation plan, and this should be included.

2) Although EEI is not permitted to ballot on these proposed changes to the CIP Reliability Standards, we note that Industry was not afforded an opportunity to vote on the proposed changes to the New, Modified and Retired NERC Glossary of Terms. Section 5.0 of the Standard Processes Manual states that “Glossary of Terms includes terms that have been through the **formal approval process**”, which EEI understands to mean that new terms are to be balloted. Therefore, the proposed terms that have been modified, added, or retired will need to be balloted prior to the final approval of the proposed CIP Reliability Standards.

3) EEI notes that acronym for Shared Cyber Infrastructure (SCI) is used prominently in many of the proposed new NERC CIP Standards but is often not identified in its first use in the following Reliability Standards. (See below)

CIP-002-7 – SCI used 27 times but never identified as Shared Cyber Infrastructure
CIP-004-Y - SCI is used 23 times but never identified as Shared Cyber Infrastructure
CIP-005-8 – SCI is used 30 times but never identified as Shared Cyber Infrastructure
CIP-006-7 - SCI is used 17 times but never identified as Shared Cyber Infrastructure
CIP-007-7 – SCI is used 23 times but never identified as Shared Cyber Infrastructure
CIP-008-7 – SCI is used 12 times but never identified as Shared Cyber Infrastructure

CIP-009-7 – SCI is used 12 times but never identified as Shared Cyber infrastructure
CIP-010-5 – SCI is used 15 times but never identified as Shared Cyber infrastructure
CIP-011-Y – SCI is used 3 times but never identified as Shared Cyber infrastructure
CIP-013-3 – SCI is used 17 times but never identified as Shared Cyber infrastructure

Likes 0	
Dislikes 0	

Response

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6

Answer	
Document Name	

Comment

Recommend spelling out “Shared Cyber Infrastructure” within CIP-002 standard text

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers these additional comments:

- Redlines to the current approved standard would be appreciated to understand the changes between current obligations and the proposed changes.
- Due to the differences in traditional and virtual technologies, the SDT should consider moving the virtual requirements to a separate standard or standards. This will reduce confusion when applying the requirements and allow those who do not plan to use virtualization to focus on the requirements relevant to them and not be distracted by terminology and requirements that do not apply to them.
- BES Cyber System definition: The proposed definition appears to require two separate groupings if SCI is in use, one for the BES Cyber Assets, and one for the Shared Cyber Infrastructure. Recommend a simplification, “One or more BES Cyber Assets logically grouped by a Responsible Entity to perform one or more reliability tasks for a functional entity, and the Shared Cyber Infrastructure supporting the BES Cyber Assets supported.”

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
None.	
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	
As pertaining to EACMS and with the broadening and nesting of definitions, the need for the EACS/EAMS split becomes more evident, and possibly even different types of EACS (or no type at all) as it appears the requirements are trying to specify requirements for firewalls as opposed to domain controllers as one example. As Zero Trust, policy enforcement within hypervisors, virtual FW's, etc. proliferate, the broad definition of EACMS as a “thing” is becoming more of an issue with virtualization. Electronic Access Control is a function and not a type of CA or VCA and virtualization and zero trust are making this ever more evident. Including logging systems that only monitor access in the same definition adds to the issue. The standards appear to begin to split this broad category with phrases like "EACMS that enforce an ESP", but that is also problematic. Domain Controllers (DC) 'enforce a policy' that can 'control communications', yet some of the requirements that use this scope can’t be applied to a DC. (CIP-005 R1.2 and R1.3 for example. R1.3 would break most systems as it could require that a virtual BCS can't talk to a DC. Although we understand the intent is to prevent virtual tenant access to the SCI management plane, it says far more due to the intertwining of definitions. This requirement says a virtual BCS on independent SCI must be prevented from communications to the Management Interface, which is defined as "a user interface that is…used to configure an ESP" which is defined as "…policies enforced by an EACMS that controls communications". The virtual BCS cannot communicate to the Domain Controller (breaking the BCS) because the DC may enforce group policy that may control communications (what ports or services are enabled/disabled on servers). Attempting to do electronic access control to an EACMS management plane is perilous with these broad constructs. "Electronic access control" is a broad function with no differentiation between IP network type access control (firewalls) and user/process authentication (domain controllers) or IRA access control (Intermediate Systems) or merely logging systems attempting to correlate events for detection. With the philosophy that every Cyber Asset or VCA is every definition it meets, this is an issue that needs simplification. Regarding the Implementation Plan, it is missing the "Planned or Unplanned Changes Resulting in a Higher Categorization" section that should be included in order to carry that forward to the new version of CIP-002. The list of definitions in the Implementation Plan needs to be updated as well.	
Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7	
Answer	
Document Name	

Comment
The SDT has been clear that this project focuses on on-premise virtualization, however, many virtualization concepts could be interpreted as being related to cloud computing technologies. AWS suggests explicitly stating that the Standards do not apply to cloud within the Applicability section of CIP-002. If these updated Standards do not apply to cloud, it should be obvious to the reader. Thank you to the drafting team for all your work.

Likes 0	
Dislikes 0	

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	
Document Name	

Comment
<duplicate>

Likes 0	
Dislikes 0	

Response

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

Comment
Although ACES answered no to question #7, an ACES member agrees with the SDT in question #7, stating they see advantages to leveraging policies in zero trust environments to reduce overall burden of documenting ESPs. Further, they feel the differences in technology between traditional perimeter controls and zero trust would not hinder the audit process.

We would like to thank the SDT for their hard work on this project and addressing industry comments. This draft is significantly closer to the existing standards while allowing the flexibility to incorporate newer and future technologies to protect the BES.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	
Document Name	NEE-20210819-Virtualization_Unofficial_Comment_Form_06302021.pdf

Comment

- The SDT has provided significant improvements in the July release yet a few clarifications are still required. We appreciate the efforts of SDT and supporting contributors.
- Of the two following examples, which diagram, if the proposed definition change of ERC is accepted, depicts the ESP network of a typical substation? (see attached)

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	
Document Name	

Comment

While GSOC understands the need for the standards and supporting technical rationale to comport to the new style and standards instituted by NERC and the contraints of format revisions, the loss of context in moving historical technical rationale supporting the standards to

'retired' status creates ambiguity. Specifically, the movement of this substantive guidance to a retired section raises questions regarding whether portions of the guidance that remain applicable and are not clearly superseded can be relied upon by industry. For theses reasons, GSOC recommends that clarification be provided regarding whether substantive guidance provided in previous versions of the technical rationale that were moved to the 'retired' section in the latest version of the technical rationale and are not clearly superseded in the substantive portions of the new/revised technical rationale remain in effect and can be relied upon and utilized by industry in their compliance efforts. This clarification is critical because the movement of substantive guidance without replacement or clear superseding information reduces the overall guidance available to entities trying to adhere to a complex set of obligations.

GSOC appreciates the SDT's efforts on these changes. The proposed revisions are a substantive improvement and should address the majority of concerns previously expressed. Overall, GSOC supports the concepts proposed in the draft revisions.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

We understand the SDT desires to allow flexibility for entity's to address a mixed trust environment, however the mixed trust environment may not be allowable based on our comments in Q1. In SDT proposed "independently Identified SCI" scenario (see the diagram in Q1), if the right side SCI containing a CIP Management Interface can remove a CIP cyber asset, the SCI should be identified as a CIP cyber asset (see our comments in Q1) resulting in all non-CIP VCAs it host becoming at least PCAs based on the affinity rule, therefore the proposed mixed trust model is broken and cannot provide flexibility for entities to achieve CIP compliance. To make the right side SCI out of CIP scope, the only way to do so is that the right side SCI cannot have a CIP Management Interface and its hosted VCAs cannot be CIP cyber assets. The only mixed trust environment can be done is the storage array. In our proposed changes, the storage array should be identified as part of the CIP cyber asset only if it contains the information for the real-time operation of a CIP cyber asset like a local hard drive and the rest of the storage array for storing historical information and non-real time information may be identified as a BCSI repository.

Entity's who choose to host both CIP and non-CIP cyber assets on SCI must understand the high security risk to the reliable operation of BES as changes to this complex environment could cause a misconfiguration, loss of service, security vulnerability or other issue which can impact the entire SCI virtual hardware platform and the hosts, VMs and their configurations. Also, resulting from our comments above, the non-CIP cyber assets on the mixed trust SCI becomes PCAs if the SCI contains CIP Management Interface in which it would bring additional compliance obligations to the Entity's who choose to do so.

Resulting from our proposed changes, the We believe the existing standard requirements and definitions could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, and reduce the impact to entity's existing CIP programs.

that affect the reliable operation of BES and provide greater clarity to auditors.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

We concur with the SDT's goal of revising the CIP standards to address virtualization, provide more options for Responsible Entities to remain compliant and ensure reliability while utilizing new and different technologies, and be objective-focused. To that end, we applaud the SDT's continued work and effort on this project. While there are several negative comments listed above, we also feel that CIP-002, 005, 007, and 010 are also close to an acceptable revised state.

While the proposed revisions are made with the intent of allowing Responsible Entities more options to achieve compliance, the inclusion of multiple new and revised terms and requirement language across all CIP requirements gives the appearance of more complexity and thus more difficulty in achieving compliance. This may (or may not) only be an issue of optics but optics are important. The goal of providing Responsible Entities more options for compliance must not also detract from the goal of ensuring that the requirements are understandable and explainable to a wide audience.

The biggest concerns with all of these changes are:

CIP-002 – How will we identify if assets are in scope with the changes made to attachment 1

CIP-010 – How the removal of baseline configurations will affect SRP-PAC

We thank the SDT for this opportunity to provide comment and feedback.

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	
Document Name	

Comment

Planned and Unplanned changes language should be added to the Implementation Plan, similar to the language included in previous CIP implementation plans. *(See Implementation Plan For Version 5 CIP Cyber Security Standards, November 7, 2011; Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012; and Implementation Plan - Project 2014-02 CIP Version 5 Revisions, January 23, 2015.)*

Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	

In support of IRC SRC/SWG.

Overall, the SRC recommends a separate virtualization standard be adopted to reduce the amount of change, additional work and confusion that will be required by a more holistic change as noted by the SDT. The new standard should be limited to only the requirements that directly relate to virtualization technology (e.g. dedicated infrastructure, shared infrastructure and management systems). In the event the SDT declines to pursue a separate virtualization standard, the SRC offers these comments in Questions 1-14 on the draft standards as presented.

Are these comments for the SAR drafting team or the Standards drafting team per the question's text?

Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries request that the SDT post the draft revisions as "red-line to last approved" rather than "to last posted." This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates.

Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?

Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 3	
Answer	
Document Name	
Comment	

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	
Response	

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	
Document Name	
Comment	
Planned and Unplanned changes language should be added to the Implementation Plan, similar to the language included in previous CIP implementation plans. *(See Implementation Plan For Version 5 CIP Cyber Security Standards, November 7, 2011; Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012; and Implementation Plan - Project 2014-02 CIP Version 5 Revisions, January 23, 2015.)*	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	
Document Name	
Comment	
Regarding new definitions, such as Cyber System and CIP System, the we requests an example collection that would meet each definition. Intermediate System? SIEM? A Venn diagram may also be useful.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Are these comments for the SAR drafting team or the Standards drafting team per the question's text? Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries Request that the SDT post the draft revisions as "red-line to last approved" rather than "to last posted." This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates. Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	

Comment
We understand the SDT desires to allow flexibility for entity's to address a mixed trust environment, however the mixed trust environment may not be allowable based on our comments in Q1. In SDT proposed "independently Identified SCI" scenario (see the diagram in Q1), if the right side SCI containing a CIP Management Interface can remove a CIP cyber asset, the SCI should be identified as a CIP cyber asset (see our comments in Q1) resulting in all non-CIP VCAs it host becoming at least PCAs based on the affinity rule, therefore the proposed mixed trust model is broken and cannot provide flexibility for entities to achieve CIP compliance. To make the right side SCI out of CIP scope, the only way to do so is that the right side SCI cannot have a CIP Management Interface and its hosted VCAs cannot be CIP cyber assets. The only mixed trust environment can be done is the storage array. In our proposed changes, the storage array should be identified as part of the CIP cyber asset only if it contains the information for the real-time operation of a CIP cyber asset like a local hard drive and the rest of the storage array for storing historical information and non-real time information may be identified as a BCSI repository. Entity's who choose to host both CIP and non-CIP cyber assets on SCI must understand the high security risk to the reliable operation of BES as changes to this complex environment could cause a misconfiguration, loss of service, security vulnerability or other issue which can impact the entire SCI virtual hardware platform and the hosts, VMs and their configurations. Also, resulting from our comments above, the non-CIP cyber assets on the mixed trust SCI becomes PCAs if the SCI contains CIP Management Interface in which it would bring additional compliance obligations to the Entity's who choose to do so. Resulting from our proposed changes, the MRO NSRF believes the existing standard requirements and definitions could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, and reduce the impact to entity's existing CIP programs. that affect the reliable operation of BES and provide greater clarity to auditors. We thank the SDT for this opportunity to provide comment and feedback. We concur with the SDT's goal of revising the CIP standards to address virtualization, provide more options for Responsible Entities to remain compliant and ensure reliability while utilizing new and different technologies, and be objective-focused. To that end, we applaud the SDT's continued work and effort on this project. While there are several negative comments listed above, we also feel that CIP-002, 005, 007, and 010 are also close to an acceptable revised state. While the proposed revisions are made with the intent of allowing Responsible Entities more options to achieve compliance, the inclusion of multiple new and revised terms and requirement language across all CIP requirements gives the appearance of more complexity and thus more difficulty in achieving compliance. This may (or may not) only be an issue of optics but optics are important. The goal of providing Responsible Entities more options for compliance must not also detract from the goal of ensuring that the requirements are understandable and explainable to a wide audience. We thank the SDT for this opportunity to provide comment and feedback.

Likes 0	
Dislikes 0	

Response
JT Kuehne - AEP - 6

Answer	
Document Name	

Comment

While AEP has provided specific commentary on Questions 1 through 13, we would like to provide the following general thoughts as revisions are incorporated.

- We ask the SDT to avoid, wherever possible, the nesting of defined terms within the definition of other defined terms. The current practice of nesting has made it difficult to support some of the great work that has already been put in by the SDT.
- AEP recommends clarifying the definitions first, then firming up CIP-002 asset classification requirements in relation to the new definitions, so that the Standards conforming to these changes can be effectively implemented.
- AEP anticipates that the outcome of this revision to the CIP standards to have significant impact on the manner by which Access Management and other tasks are performed. For example, this will require the development of controls in the areas of electronic access authorizations, reviews, revocations etc., related to BCSInfo on SCI. As such, we suggest SDT provides clarifications on the new and revised definitions as requested.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	
Document Name	

Comment

In support of NPCC RSC comments.

Are these comments for the SAR drafting team or the Standards drafting team per the question’s text?

Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries

Request that the SDT post the draft revisions as “red-line to last approved” rather than “to last posted.” This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates.

Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	

Document Name	
Comment	
Planned and Unplanned changes language should be added to the Implementation Plan, similar to the language included in previous CIP implementation plans. *(See Implementation Plan For Version 5 CIP Cyber Security Standards, November 7, 2011; Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012; and Implementation Plan - Project 2014-02 CIP Version 5 Revisions, January 23, 2015.)*	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	
Document Name	
Comment	
OKGE supports EEI's comments especially in regards to the proposed new and modified terms that are not being balloted.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	2016-02_Virtualization_Unofficial_Comment_Form_R2_RF_FINAL.docx
Comment	
See Question 14 in the attached document	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	

Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	
Document Name	
Comment	
We support NPCC TFIST's comments as found below: Are these comments for the SAR drafting team or the Standards drafting team per the question's text? Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries Request that the SDT post the draft revisions as "red-line to last approved" rather than "to last posted." This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates. Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	

Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	
Document Name	
Comment	
Because the Technical Rationale documents are being removed from the Standard template, we would suggest that links to these documents be incorporated into each Standard for ease of reference.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	
Document Name	
Comment	
BC Hydro welcomes the opportunity to comment and expresses gratitude for SDT's efforts to continue to move towards a practical and industry-wide acceptable solution to the technical question of Virtualization faced by the Entities in the NERC CIP domain. BC Hydro looks forward to the enhancements of the identified items in glossary of terms for a better understanding and successful implementation.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not agree all proposed changes are specific to virtualization. The revisions to CIP-010 R1.1, for example, are not clear how removing the requirement to maintain baseline documentation is related to permitted virtualization architecture or the security risks associated with virtualization technologies. Texas RE respectfully requests the SDT’s reasoning for how each of the proposed changes address security risks and permitted architecture specific to virtualization.	

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	
Document Name	

Comment

SIGE proposes the following for CIP-003 Attachment 1 Section 5, 5.1 and 5.2.

“Controls that maintain the state of the operating system and software such that it is in a known state prior to use;”

In CIP-006, in the Applicable Systems column for Part 1.1, the term “hosting” is used in “SCI without ERC hosting Medium Impact BCS,” but “hosting” has been changed to “supporting” in other places.

Similarly, in CIP-009, in the Applicable Systems column for Parts 2.1 and 2.2, the term “hosting” is used in “SCI hosting Medium Impact BCS at Control Centers or their” but “hosting” has been changed to “supporting” in other places.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)

Answer	
Document Name	

Comment

SPP wants to thank the drafting team for their work on these proposed revisions.

Recommend correcting the spelling error in CIP-005 2.6.2 “systerms” should be “systems”.

Recommend spelling the SCI acronym out on page 5 since it is the first use of the term.

Recommend changing reference “1.4” to “1.3” on page 32 under the VSL section.

Recommend researching and adding in the word “Cyber” in all areas that reference “Cyber Security Patch” for document consistency.

Likes 0	

Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	
Document Name	

Comment

CEHE proposes the following for CIP-003 Attachment 1 Section 5, 5.1 and 5.2.

“Controls that maintain the state of the operating system and software such that it is in a known state prior to use;”

In CIP-006, in the Applicable Systems column for Part 1.1, the term “hosting” is used in “SCI without ERC hosting Medium Impact BCS,” but “hosting” has been changed to “supporting” in other places.

Similarly, in CIP-009, in the Applicable Systems column for Parts 2.1 and 2.2, the term “hosting” is used in “SCI hosting Medium Impact BCS at Control Centers or their” but “hosting” has been changed to “supporting” in other places.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	
Document Name	

Comment

We concur with the SDT’s goal of revising the CIP standards to address virtualization, provide more options for Responsible Entities to remain compliant and ensure reliability while utilizing new and different technologies, and be objective-focused. To that end, we applaud the SDT’s continued work and effort on this project.

With that said, after considerable time reviewing the proposed revisions and additions, and much time consulting with and debating peers over the changes, we have arrived at the conclusion that it might be a mistake to attempt virtualization solely through revision of the existing CIP requirements. Currently the revisions are focused on setting the requirements at a level high enough to be technology agnostic, where they can be applied regardless of whether a mixed-trust approach is used. While laudable in theory, the result so far seems to be extensive revisions requiring multiple new definitions, all of which are somewhat confusing in their entirety and potentially difficult to implement properly due to the confusion. Further the extent of the changes presents opportunities for auditors in future to arrive at undesired intepretations. Compounding the issue is that these changes are being made to allow for options which not all Responsible Entities will avail themselves of – and in fact possibly very few will, at least in the near future. Again, we support the SDT’s goal of allowing Responsible Entities more options for maintaining reliability and compliance. But we question how worthwhile it is to enact a raft of changes on existing requirements where only a minority of companies will be seeking to use them.

Accordingly, instead of revising every existing CIP requirement, we believe that a new CIP standard should be enacted, along with any necessary changes to CIP-002 R1 for scope and CIP-005 R1 for ESP, to address virtualization requirements. This can meet all the goals of the SDT while minimizing impact to existing CIP requirements and compliance programs.

We thank the SDT for this opportunity to provide comment and feedback.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	
Document Name	

Comment

We would like to thank the SDT for their hard work on this project and addressing industry comments.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	
Document Name	

Comment

This approach is highly based on a Zero Trust Model. While Zero Trust and it's assumption of assuming no network edge is an excellent security approach, it is necessary to ensure that a discrete boundary defines the edge of the auditable network. The current definitions significantly blur this border introducing uncertainty into what will be audited under the CIP standards and introduces opportunity for significantly different viewpoints between auditors and entities regarding the boundary of what will be subject to NERC compliance standards. The definitions are also too dependent on interpretation that is not enforceable as the appropriate guidelines are no longer a part of the standard. We do support adopting definitions and standards that support virtualization.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	
Document Name	
Comment	
AZPS would like clarification on the PCA Definition regarding the phrase “actively remediated” and what that entails?	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	
‘Where technically feasible’ -> ‘Per system capability’ **MRO Comment:** There are instances of ‘per system capability’ replacing ‘where technically feasible’ that could allow for fewer protections for those BCS. The ROP requires that TFEs require “Compensating and mitigating measures” (NERC ROP Appendix 4D). This is no longer required and limits compliance monitoring. (Consider an EACMS or PACS, which do not require logical isolation, not requiring authentication [Part 5.1] or limiting authentication attempts [Part 5.7]. This poses an increased risk.) **Recommendation:** Modify the language of the requirements beyond just replacing ‘where technical feasible’ with ‘per system capability’ to better address risk posed by the lack of the required controls.	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	
Document Name	
Comment	
Additional minor and conforming recommendations: CIP-006 Table R2 part 2.2 - Under Applicable Systems, typo, "EERC" meant to be read as ERC.	

CIP-006 Table R3 part 3.1 - Under Applicable Systems, consider removing bulleted SCI applicability and include as a single statement at the bottom of the column for consistency.
CIP-007 Table R1 part 1.3 & Table R4 part 4.2 - Under Applicable Systems, the second bullet "External Routable Connectivity" can be changed to ERC for consistency.
CIP-009 Table R2 part 2.1 & 2.2 - Under Applicable Systems, to improve clarity consider removing 'SCI hosting High or Medium Impact BCS at Control Centers or their associated EACMS/PACS' as these would be included in High and Medium impact BCS in an All-In scenario while 'SCI identified independently supporting an Applicable System Above' covers the independently identified scenario.

Likes 0	
Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5

Answer	
Document Name	

Comment

We concur with the SDT's goal of revising the CIP standards to address virtualization, provide more options for Responsible Entities to remain compliant and ensure reliability while utilizing new and different technologies, and be objective-focused. To that end, we applaud the SDT's continued work and effort on this project. While there are several negative comments listed above, we also feel that CIP-002, 005, 007, and 010 are also close to an acceptable revised state.

While the proposed revisions are made with the intent of allowing Responsible Entities more options to achieve compliance, the inclusion of multiple new and revised terms and requirement language across all CIP requirements gives the appearance of more complexity and thus more difficulty in achieving compliance. This may (or may not) only be an issue of optics but optics are important. The goal of providing Responsible Entities more options for compliance must not also detract from the goal of ensuring that the requirements are understandable and explainable to a wide audience.

We thank the SDT for this opportunity to provide comment and feedback.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	

Comment
CIP-005-8 R1.2 – Has been revised to incorporate requirements for "controlled communications" to and from Management Interfaces. Additional clarity should be provided for the "controlled communicaiton" concept, as currently drafted there is an elevated risk of incorrect implementation by entities due to not adequately interpreting the requirement. CIP-005-8 R2.6.2 - Has been revised to incorporate requirements for "controlled communications" to and from Management Interfaces. Additional clarity should be provided for the "controlled communicaiton" concept, as currently drafted there is an elevated risk of incorrect implementation by entities due to not adequately interpreting the requirement. CIP-007-7 R4.1 - The SDT may have struck necessary language when “at the BES Cyber System level (per BES Cyber System capability) or a the Cyber Asset level (per Cyber Asset capability) was removed from CIP-007-6.

Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	
Document Name	

Comment
Duke Energy appreciates the efforts of the SDT to continue to incorporate feedback and drive towards an implementable, sustainable set of requirements and definitions. Duke has proposed a number of definition changes that we believe are foundational to the success of this effort. Duke Energy is voting negative on the non-binding poll related to the VRFs and VSLs based on the dependency on definitions and other related comments captured in comment submittals for questions 1 – 13.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	

Document Name	
Comment	
Xcel Energy thanks the drafting team for their hard work and dedication to making the utilization of virtualized systems in CIP environments more effective and flexible. We generally support your efforts and believe the team is on the right track.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	
Document Name	
Comment	
The trend with the CIP standards has been to change from requiring a specific control to address a cyber security objective to requiring the RE to achieve a cyber security objective. For example, in CIP-007-3, the RE was required to implement antivirus on in-scope CAs to mitigate the threat of malicious software. CIP-007-5 changed this to require the RE to deploy methods to deter, detect or prevent malicious code. This gave the RE the ability to choose the best control for the actual objective (malicious code protection) as opposed to requiring the entity to implement specific control (antivirus) that may not be suitable in all cases. The same can be said for the proposed revisions to ESPs, rather than requiring the specific control of firewalls to act as EAPs for an ESP, the SDT is revising the requirement to grant the RE the ability to select the control best suited to their environment to achieve the cyber security objective (logical isolation). The SDT should use the same objectives based approach with side-channel threats and create requirements that require the RE to design and implement controls that mitigate the threat of side-channel attacks, rather than force entities to implement the specific control of CPU/memory isolation, which is certainly one option, but not the only one. Other controls that would be effective is network isolation of the SCI and its VCAs, whitelisting, or more organizational control to prevent information disclosure (such as randomizing data in memory). Additionally, the CIP standards already address several of the most important controls to prevent side-channel attacks, namely, regular security patching, ports and services hardening, and restricting user access based on need.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
Reclamation appreciates the SDT’s efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the SDT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	Dominion Enegy additional Virtualization comments.docx
Comment	
Please see the attached file with graphics.	
Likes 0	
Dislikes 0	
Response	

Comments Submitted by Lakeland Electric (JEA was originally expected to submit these comments)

1. Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

☒ Yes
☐ No

Comments: **look at applicability

2. The Applicable Systems column may include "SCI identified independently…" Is this clear or is additional clarification (such as "SCI identified as supporting, but not part of…") needed?

☐ Yes
☒ No

Comments: Need to combine and include both (because 'independently' is listed throughout standards and needs to be defined). Example: "SCI identified IDENPENDENTLY as supporting, but not part of…."

3. The SDT modified the ERC definition to reference "outside the asset containing". This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: This definition of ERC (by including the new definition of CIP System) extends ERC requiremetns to EACMs and PACs and transient cyber assets. Should be limited to environments that control and monitor BES.

4. The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: As the proposed change extends ESP application to CIP Systems (which include EACMs and PACs and transient cyber assets). This application of ESP must be limited to assets impacting BES Control and Monitoring Operations.

5. The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: IRA definition is applied to CIP Systems which requires application of IIRA to TCA, EACMS, and PACS

6. The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: Is Management interface the Virtual Management Consoles or ILO.

7. As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments:

8. The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: Deviates from industry standard terms such as used in NIST.

9. The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: No value addition to current CIP process and adds confusion to CIP asset identification process. If the intent is just clarify VCA, then adding the definition should be more than sufficient.

10. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: No value addition to current CIP process and adds confusion to CIP asset identification process. If the intent is just clarify VCA, then adding the definition should be more than sufficient.

11. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP-007 requirements and improve to risk based compliance.

12. The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP-010 requirements and improve to risk based compliance.

13. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP requirements and improve to risk based compliance.

14. Please provide any additional comments for the SAR drafting team to consider, if desired.

Objective of this SAR was to improve CIP standards to allow use of new technologies such as Cloud where appropriate and improve CIP compliance. Unfortunately, this standard stifles any innovation and forces the industry to use obselence.

- SDT classifies all CIP standards as same risk, which defeats the objective of creating a risk based compliance program.
- Adds a level of complexity and a lack of clarity that would make implementation difficult and result in increased violations without an increase in security.
- Move away from risk-based standards by not segregating assets (such as EACMS, PACS, and TCA) in definitions such as those for CIP System and ERC.
- Do not accomplish the goal and deviate from the original purpose of the SAR: to eliminate the language inherent in V5 that has made it difficult to go virtual. In fact, they may limit or handicap an entity's ability to go virtual.
- This standard does not add any value to CIP standards as all what is being accomplished by these changes can easily be accomplished by current standards. If the intent is to clarify the application of Virtual systems, then SDT or ERO should release an application white paper.

Comments Submitted by Orlando Utilities Commission (JEA was originally expected to submit these comments)

1. Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

☒ Yes
☐ No

Comments: **look at applicability

2. The Applicable Systems column may include “SCI identified independently…” Is this clear or is additional clarification (such as “SCI identified as supporting, but not part of…”) needed?

☐ Yes
☒ No

Comments: Need to combine and include both (because ‘independently’ is listed throughout standards and needs to be defined). Example: “SCI identified IDENPENDENTLY as supporting, but not part of….”

3. The SDT modified the ERC definition to reference “outside the asset containing”. This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: This definition of ERC (by including the new definition of CIP System) extends ERC requiremetns to EACMs and PACs and transient cyber assets. Should be limited to environments that control and monitor BES.

4. The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: As the proposed change extends ESP application to CIP Systems (which include EACMs and PACs and transient cyber assets). This application of ESP must be limited to assets impacting BES Control and Monitoring Operations.

5. The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: IRA definition is applied to CIP Systems which requires application of IIRA to TCA, EACMS, and PACS

6. The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: Is Management interface the Virtual Management Consoles or ILO.

7. As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments:

8. The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: Deviates from industry standard terms such as used in NIST.

9. The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: No value addition to current CIP process and adds confusion to CIP asset identification process. If the intent is just clarify VCA, then adding the definition should be more than sufficient.

10. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: No value addition to current CIP process and adds confusion to CIP asset identification process. If the intent is just clarify VCA, then adding the definition should be more than sufficient.

11. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP-007 requirements and improve to risk based compliance.

12. The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP-010 requirements and improve to risk based compliance.

13. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP requirements and improve to risk based compliance.

14. Please provide any additional comments for the SAR drafting team to consider, if desired.

Objective of this SAR was to improve CIP standards to allow use of new technologies such as Cloud where appropriate and improve CIP compliance. Unfortunately, this standard stifles any innovation and forces the industry to use obselence.

- SDT classifies all CIP standards as same risk, which defeats the objective of creating a risk based compliance program.
- Adds a level of complexity and a lack of clarity that would make implementation difficult and result in increased violations without an increase in security.
- Move away from risk-based standards by not segregating assets (such as EACMS, PACS, and TCA) in definitions such as those for CIP System and ERC.
- Do not accomplish the goal and deviate from the original purpose of the SAR: to eliminate the language inherent in V5 that has made it difficult to go virtual. In fact, they may limit or handicap an entity's ability to go virtual.
- This standard does not add any value to CIP standards as all what is being accomplished by these changes can easily be accomplished by current standards. If the intent is to clarify the application of Virtual systems, then SDT or ERO should release an application white paper.

Overall Comments:

The June 2021 redlines are an improvement over the previous version; however, the modifications:

- Add a level of complexity and a lack of clarity that would make implementation difficult and result in increased violations without an increase in security.
- Move away from risk-based standards by not segregating assets (such as EACMS, PACS, and TCA) in definitions such as those for CIP System and ERC.
- Do not accomplish the goal and deviate from the original purpose of the SAR: to eliminate the language inherent in V5 that has made it difficult to go virtual. In fact, they may limit or handicap an entity's ability to go virtual.
- This standard does not add any value to CIP standards as all what is being accomplished by these changes can easily be accomplished by current standards. If the intent is to clarify the application of Virtual systems, then SDT or ERO should release an application white paper.

- Definitions
- **CIP System** - this extends the definition to include EACMS, PACS, and TCA. When applied in standards or other definitions, it expands the scope significantly. Systems such as SIEM and PACS are supposed to control and Monitor an enterprise and separate instances limit the ability of security operations to respond to active incidents. Applying CIP System definitions will expand scope to environments where impact will limit security and will be detrimental.
- We recommend this definition be removed and appropriate devices groups such as EACMs, PACS be directly used in order to avoid any confusion.
- **ERC** – by including "ability to connect to a CIP System," in the definition of ERC, this extends ERC requirement to EACMS, PACS, and TCA. Should be limited to environments that control and monitor BES as was the scope of the SAR. Also, the statement "outside the asset containing the CIP system" may need clarity – where does this draw the line? **ESP** – as proposed, it appears this may extend the definition of ESP to CIP Systems (including EACMS, PACS, and TCA), but application of ESP must be limited to assets impacting BES control & monitoring operations. EACM, PACS and TCA should not be required to maintain an ESP as they are support assets and exists in homogeneous corporate environment. This change assumes the same risks for all assets/environments and fails to deliver a Risk based application.
- **Intermediate Systems** – should not be on the same network for which it restricts the access or any of the devices it protects. This definition is understood.
- **IRA** – Does this now apply to all within ESP and IRA applies to any of the CIP Systems? Why does the last bullet so specific and not make reference to "asset point?" Overall, definition is understood, but complicated.
- **Management Interface** – we need more clarity, for example does this include ILO as management interface? Is it a vector or device (ESXI console)?

- **TCA** – this definition/inclusion of the virtual environment is confusing. If the TCA is on the same network, then it will bea PCA or if separate then it will have to use a jump host. How will this apply to Entity's virtual workstations? Would we have to prove the virtual system has ESP and ERC compliance? Need clarity.

- CIP-002
  - It is clear that we are given two options: (1) SCI included in CIP Systems and treated as the[MDD-DCC1] CIP System; and (2) SCI identified independently; just to be clear, based on "each asset", are we also able to do a hybrid model in which some SCI is include and some SCI is identified as independent? It appears to be the case.
  - New standard allows for either zero trust method (protect close to asset) or former edge-based method (ESP and firewalls); however if we want to continue with the edge-based method, we don't want to high water mark everything
    - i.e. Does this mean the corporate host may become SCI for CIP?
    - That CIP System is really giving us a problem in terms of ERC
  - We have concern that corporate host may become SCI; Will the SIEM systems (EACM) not allowed to share Processor and Memeory, that would require them to maintain separate SCI and hence critical requirements such as SIEM can never be migrated to Cloud instance and can never take advantage of any new technology. Furthermore, such a standard assumes that Risks for the EACM and BES assets is exactly the same, and fails to deliver a Risk based application which was the FERC manadate. SDT can specify the security requirements for Shared SCI in a manner that addresses the risk and hence allowing Entities to benefits from transitioning to more advanced technology for EACMs and Data storage, which will significantly improve security.

- CIP-005
  - Allows us to keep firewall or take protection closer to the asset
  - Part 1.2 – only applies to firewall because "identified independently"
  - Part 1.4 – addresses ability to have a "super ESP" between 2 control centers and protect communication between the two
  - Part 2 – ok with requirement; but is there any other way for vendors to access that doesn't involve intermediate host?

- CIP-007
  - Part 1.1 – if this requires EACMS connect to TCA, we may have a problem – includes EACMS, PACS, & PCA except we've high water marked our PACS as high
    - What is meant by "or services if unable to determine ports" – is this for dynamic port ranges or for cloud services to randomly change ports?
  - Part 1.2 – "non-programmable communications components inside PSP & ES," what is this? Is this encouraging USB port locks?
  - Part 1.4 – If you choose independent SCI, can't run ES Cyber systems along with non-CIP
    - NOTE: JEA does not agree the requirements are risk-based.; should be differentiated because this limits our availability to use virtual technology
    - How can we verify that memory is not shared?

- CIP-010
  - Need to review

- CIP-011
  - Ok for the most part