Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization
Comment Period Start Date:	1/22/2021
Comment Period End Date:	3/22/2021
Associated Ballots:	2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 IN 1 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 IN 1 ST

There were 91 sets of responses, including comments from approximately 210 different people from approximately 133 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT added, revised, and retired 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.

2. CIP-005 Requirement R1 part 1.1 was revised to permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

4. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.

5. The SDT modified CIP-005 Requirement R2 to ensure remote access management requirements align with the new and revised virtualization terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

6. The SDT revised CIP-007 Requirement R1 Part 1.1 to shift the security objective from logical network accessible ports to services. The proposed revisions require Responsible Entities to enable only network accessible services that have been determined to be needed by the Responsible Entity. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

7. CIP-010 Requirement R1 currently requires Responsible Entities to develop a baseline configuration, authorize changes to the baseline, and document the changes. The SDT proposes to revise Requirement R1 to remove the reference to baseline configurations. The proposed revisions require the authorization of changes to Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible ports, security patches applied, and SCI configurations. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

8. The SDT modified CIP-010 Requirement R3 Part 3.3 to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. The revised requirement allows the use of remediation VLANs to perform active vulnerability assessments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

9. CIP-002-5.1a includes exemption 4.2.3.2, which exempted Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. In the development of conforming changes, the SDT determined that the exemption should be split into two distinct exemptions to adequately cover all cyber systems associated with conforming changes. The SDT

established those conforming changes in proposed Exemptions 4.2.3.2 & 4.2.3.3. Do the changes clearly identify the exempted cyber systems? If not, please provide the basis for your disagreement and an alternate proposal.

10. BCS and SCI are mutually exclusive by definition, however SCI poses a significant reliability risk to the Bulk Electric System. The SDT considered the risks associated with SCI and revised CIP-002 Requirement R1 to include the identification of SCI in Parts 1.3, 1.4, and 1.5. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

11. In the current enforceable standards, there are no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement. The SDT revised CIP-002 to include the identification of SCI associated with EACMS, PACS, and PCAs to help address this issue within the virtualization scope of the current SAR. The proposed requirement could reduce possible non-compliance to a single issue if a Responsible Entity fails to properly identify SCI associated with EACMS, PACS, or PCAs. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

12. The SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved Request for Interpretation (RFI) regarding "shared BES Cyber Systems." The SDT modified the criterion to reference each discrete shared BCS. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

13. The SDT made conforming changes to CIP-003 and CIP-004. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

14. The SDT modified the Applicable Systems column in CIP-006 to include SCI hosting PACs associated with Medium Impact BCS with ERC or IRA. The SDT made the proposed revisions to clarify the scope of requirements that apply when an entity implements serial IRA. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

15. The SDT made conforming changes to CIP-008 and CIP-009. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

16. The SDT modified CIP-011 Requirement R2 part 2.1, which will allow cryptographic erasure in scenarios where BCSI can't be mapped to particular disks in virtualized storage. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

17. The SDT performed a review of the CIP Standards and determined that CIP Exceptional Circumstances could be applied to the following additional requirements: CIP-004-7 Requirement R2 Part 2.2, CIP-004-7 Requirement R3 Part 3.5, CIP-006-7 Requirement R1 Part 1.8, CIP-006-7 Requirement R1 Part 1.9, CIP-006-7 Requirement R2, CIP-010-5 Requirement Part 1.2, and CIP-010-5 Requirement R1 Part 1.3. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

18. Implementation Plan: The SDT proposes an Implementation Plan that makes the revised CIP Standards and definitions effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order. However, the implementation plan allows a Responsible Entity to elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. Do you agree with this proposal? If you think an alternate effective date is needed, please provide a detailed explanation of actions and time needed.

19. Please provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2016-02 Virtualization	Bobbi Welch	MISO	2	RF
					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
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Michael DelViscio	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
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
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
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					David Hartman	Arizona Electric Power Cooperative	1	WECC
					Jennifer Bray	Arizona Electric Power	1	WECC

						Cooperative, Inc.		
DTE Energy - Detroit Edison Company	Karie Barczak	3		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
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
					Douglas Webb	Evergy	1,3,5,6	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
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		CHPD	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Ginette Lacasse	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
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	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
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated	6	NPCC

						Edison Co. of New York		
					Sean Bodkin	Dominion - Dominion Resources, Inc.	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
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable

					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
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
Associated Electric Cooperative, Inc.	Todd Bennett	3			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. The SDT added, revised, and retired 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.

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not generally agree with the proposed modifications. The definitions as currently drafted introduce a complex and difficult matrix of possible “device” identifications that are theoretically mutually exclusive (Cyber Asset, Virtual Cyber Asset, Shared Cyber Infrastructure, Management Modules) and that must then be assigned one or many “roles” (BCA, EACMS, etc.). It may be more straightforward to update the Cyber Asset definition to accommodate multiple technologies including physical or virtual components that comprise the a device (such as hardware, software, and data). The VCA definiation may not be needed if this concept is added to the definition of Cyber Asset. This would avoid introducing another device ‘type’ that is not currently included in applicability statements.

We have concerns that the definition of Management Module may apply to substation devices that have no relationship to virtualiztion. Is the intent to confine use of this term to SCI only? This question may highlight a concern with the approach of defining terms that can only be understood when read in context of the applicability statements.

The proposed definition of Self-Contained Application includes terms such as “isolated” that could be interpreted by regional entities to mean that they would not be allowed network connectivity. Most containers inherently need a network address to perform their purpose. We suggest revising the definition to something like “Packaged software, consisting of binaries that cannot be modified, containing application software, operating system, and all relevant dependencies designed to execute independent of any other software or containers residing on the same infrastructure. SCA may exist on Cyber Assets, VCA, or SCI.”

Duke recommends the SDT add a definition of ‘Logical Isolation’, as that term is central to multiple requirements.

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

TVA has concerns with the Share Cyber Infrastructure (SCI) definition: As currently drafted, this term is too vague and could be misinterpreted to extend scope inappropriately.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

SRP would like clarification on the mixed use of CIP and non CIP assets. What components within virtualization becomes an EACMS? Requirements R1 Parts 1.1, 1.2, and 1.3 are a big step from referencing an Electronic Access Point (EAP).

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: The MRO NSRF believes the existing standard requirements could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, reduce the impact to entities' programs, and provide greater clarity to auditors. We recommend reviewing our comments in reply to Question 19 first. This provides an overview basis for our comments in general.

A. SCI - Virtual environments could reside within specified physical security zones thus eliminating the need for a Shared Cyber Infrastructure (SCI) definition. For example, a BCA and PCA supported by the same hardware (server farm, storage system, management system) could be classified as a BCA (high watermarked). Using this logic also eliminates the need to retire the Electronic Security Perimeter (ESP) definition and results in less impact to entities.

B. Logical Isolation - is problematic in that it is undefined. The existing term 'routable protocol' becomes obsolete when 'logical isolation' is used as or in place of an ESP – i.e., to establish an electronic security zone. Logical isolation can expand compliance scope by bringing in non-routable serial connections.

C. VCA - Given no existing specific requirements for a VCA, the SDT could consider modifying the definition of Cyber Asset to include the entire hardware platform hosting the virtual machines. This allows entities to identify and address the appropriate CIP security risks for virtual machines. This also eliminates the need for the term VCA throughout the standards and other definitions, and in entity compliance documentation and processes.

D. Categorization - If an SCI, Management System or Management Module, such as hypervisor host and vCenter, can create, modify, delete or turn off a BCA, it should be identified and categorized in its entirety as a BCA, because it would have an adverse impact on the Bulk Electric System within 15 minutes. Entities whom choose to put many systems in one hardware platform may consider the risks associated with combined systems.

E. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off an EACMS or PACS, it should be identified as EACMS or PACS since it can remove or change the electronic/physical access control functions. This is implied but not clearly stated in the current definition. For clarity, we suggest addressing this gap by modifying the existing definitions of EACMS and PACS.

F. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off a BCA and EACMS, it should be identified as a BCA for the highest-level protection or identified with dual classifications to meet the requirements of both a BCA and EACMS.

Additional Comment: The definition of 'Self-Contained Applications' is problematic in that the current phrase "packaged to execute in an isolated environment" could scope OS installed and managed applications that use a form of virtual isolated containers such as Java Runtime Environment (JRE) that commonly runs an isolated JVM (java virtual machine) that allows local Java code to be compiled into Java Bytecode.

Recommendation: Self-Contained Applications are immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment and **are managed via Management Systems**.

G. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off an EACMS and PACS, the multiple classifications should apply. It should be identified as both an EACMS and PACS and meet requirements of both. The ability for dual classification already exists in the current version. For example, when an EACMS device is located inside an ESP, this device would be also a PCA and should meet the requirements of both EACMS and PCA.

H. Categorization - Where a storage array (raid) is using data and/or information to operate CIP Cyber Assets (rather than solely for backup), the storage array should be identified as a component of the CIP Cyber Asset and meet the same classification as the CIP Cyber Asset. This is a logical conclusion given a CIP Cyber Assets is inoperable without the storage array information and/or data. For mixed trust environments, the high-water marking rule should apply. To keep the storage raid hosting non-CIP data out of CIP scope, non-CIP storage media should be isolated or separated.

RECOMMENDATIONS - Modifications to Existing Definitions (Cyber Asset (CA), EACMS and PACS):

We recommend modifying the definitions of Cyber Asset, EACMS and PACS to eliminate the definitions of SCI, Management System and Management Modules and recommend:

- **Cyber Asset (CA):** Programmable electronic devices, including the hardware, software, and data in those devices. This includes platforms operating virtual machines, which are logical instances of an operating system or firmware hosted on a physical platform.
- **EACMS:** 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 the Cyber Assets that can create, modify, delete or turn off the above Cyber Assets.
- **PACS:** 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 the Cyber Assets that can create, modify, delete or turn off the above Cyber Assets.

SDT INTENT - Clarity is needed regarding the modifications to definitions of ERC, IRA, IS, PCA, and the retirement of ESP and EAP.

A. If the SDT intended to include non-ESP ERC, modifications to existing ERC definition should include ESP and non-ESP ERC to make it compatible with the existing requirements.

B. If the SDT intended to include non-routable IRA access, a minor modification to the existing IRA can achieve the goal. Actually the current IRA definition has already covered the serially connected devices outside of ESP resulting from (1) the current IRA definition only states the user-initiated access using a routable protocol and doesn't say all communication sessions need to be routable all the way until the end device, and (2) it doesn't say the Cyber Asset that is accessible by a remote client has to be within an ESP. For instance, when a device serially connected to a terminal server and it can be accessible by a remote client, it meets current IRA definition, but current CIP-005-5 R2 doesn't address IRA definition since it only apply to BCS with ERC and missed the serial connected devices.

However, the current CIP-004 R5.1 has implied an IRA definition (for terminations) applies to non-routable EACMS and PACS, where CIP-004 R5.1 requires entities to revoke IRA access to high and medium impact BCS w/ERC and associated EACMS and PACS, it implies EACMS or PACS may have IRA access even though they may not within an ESP- meaning not routable – but you have to revoke the IRA access to them. We suggest

changes to IRA to make it clear that the initial access using routable protocol is one of the IRA qualifiers, where the rest of the remote access session can be non-routable.

C. Given the proposed modifications to EACMS listed in this document, the current IS definition could remain unchanged.

D. Definition of ESP and EAP should not be retired since they are still an effective approach for the network perimeter level security controls for physical and virtual machines. Logical isolation is not a defined term is very subjective. If the SDT intended to allow Cyber Asset level security controls, such as using local policies based firewalls, it should be an alternative measure rather than eliminating ESP and EAP approach.

E. If the SDT intended to include non-ESP PCAs, our proposed modifications to PCA can meet SDT's goal.

RECOMMENDATIONS - Modifications to ERC, IRA, and PCA:

- **ERC:** The ability to access a BCS from a Cyber Asset that is outside of the Electronic Security Perimeter in which the BCS resides via a bi-directional routable protocol connection, or the ability to access a BCS that is not within any ESPs from a Cyber Asset through an EACMS controlling communications to and from the BCS via a bi-directional routable protocol connection.
- **IRA:** User-initiated interactive access by a person employing a remote access client or other remote access technology. Remote access originates from a Cyber Asset, using a routable protocol, that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.
- **PCA**: One or more Cyber Assets (1) that are connected to a BCS using a routable within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP; or (2) that are connected to a BCS using a routable protocol where an ESP model is not used and doesn't pass through any EACMS controlling communications to and from the BES Cyber System. The impact rating of Protected Cyber Assets is equal to the BCS it is connected to; (3) that share CPU or memory with a BCA, EACMS or PACS. The impact rating of Protected Cyber Assets is equal to the above highest rated Cyber Asset that shares CPU or memory with the Protected Cyber Assets.

Additional Comment: The proposed definition for IRA does not account for serial connections that have the only user connection point within a PSP and cannot be moved outside of the PSP.

Recommendation: IRA: If the proposed definition for IRA in Question 1 section B of the modifications to definitions of ERC and IRA is not accepted, then there should be an exception included for communications that can only originate within a PSP.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

The proposed definitions are used to significantly expand the number of “Applicable Systems” within the CIP Standards. This leads to a complex applicability section within already complex subject matter. Some of the proposed definitions are mutually exclusive, while multiple proposed terms can apply to a device’s role within the standards. The proposed definitions shift from concepts that are understood by subject matter experts and compliance staff alike, to definitions that are not clear to subject matter experts. The SDT has proposed the retirement of well-known terms such as EAPs and ESPs and added definitions with terminology that includes immutable software binaries, logical instance, and logical isolation. The proposed definitions do not provide industry with a clear understanding of cyber asset applicability. Additionally, the SDT should consider defining logical isolation due to its pervasive use throughout the proposed definitions.

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

Comments: WAPA believes the existing standard requirements could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, reduce the impact to entities’ programs, and provide greater clarity to auditors. We recommend reviewing our comments in reply to Question 19 first. This provides an overview basis for our comments in general.

1. SCI - Virtual environments could reside within specified physical security zones thus eliminating the need for a Shared Cyber Infrastructure (SCI) definition. For example, a BCA and PCA supported by the same hardware (server farm, storage system, management system) could be classified as a BCA (high watermarked). Using this logic also eliminates the need to retire the Electronic Security Perimeter (ESP) definition and results in less impact to entities.

2. Logical Isolation - is problematic in that it is undefined. The existing term ‘routable protocol’ becomes obsolete when ‘logical isolation’ is used as or in place of an ESP – i.e., to establish an electronic security zone. Logical isolation can expand compliance scope by bringing in non-routable serial connections.

3. The definition of ‘Self-Contained Applications’ is problematic in that the current phrase “packaged to execute in an isolated environment” could scope OS installed and managed applications that use a form of virtual isolated containers such as Java Runtime Environment (JRE) that commonly runs an isolated JVM (java virtual machine) that allows local Java code to be compiled into Java Bytecode.

Self-Contained Apps Recommendation: Self-Contained Applications are immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment and **are managed via Management Systems**.

VCA - Given no existing specific requirements for a VCA, the SDT could consider modifying the definition of Cyber Asset to include the entire hardware platform hosting the virtual machines. This allows entities to identify and address the appropriate CIP security risks for virtual machines. This also eliminates the need for the term VCA throughout the standards and other definitions, and in entity compliance documentation and processes.

1. Categorization - If an SCI, Management System or Management Module, such as hypervisor host and vCenter, can create, modify, delete or turn off a BCA, it should be identified and categorized in its entirety as a BCA, because it would have an adverse impact on the Bulk Electric System within 15 minutes. Entities whom choose to put many systems in one hardware platform may consider the risks associated with combined systems.

2. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off an EACMS or PACS, it should be identified as EACMS or PACS since it can remove or change the electronic/physical access control functions. This is implied but not clearly stated in the current definition. For clarity, we suggest addressing this gap by modifying the existing definitions of EACMS and PACS.

3. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off a BCA and EACMS, it should be identified as a BCA for the highest-level protection or identified with dual classifications to meet the requirements of both a BCA and EACMS.

4. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off an EACMS and PACS, the multiple classifications should apply. It should be identified as both an EACMS and PACS and meet requirements of both. The ability for dual classification already exists in the current version. For example, when an EACMS device is located inside an ESP, this device would be also a PCA and should meet the requirements of both EACMS and PCA.

5. Categorization - Where a storage array (raid) is using data and/or information to operate CIP Cyber Assets (rather than solely for backup), the storage array should be identified as a component of the CIP Cyber Asset and meet the same classification as the CIP Cyber Asset. This is a logical conclusion given a CIP Cyber Assets is inoperable without the storage array information and/or data. For mixed trust environments, the high-water marking rule should apply. To keep the storage raid hosting non-CIP data out of CIP scope, non-CIP storage media should be isolated or separated.

RECOMMENDATIONS - Modifications to Existing Definitions (Cyber Asset (CA), EACMS and PACS):

We recommend modifying the definitions of Cyber Asset, EACMS and PACS to eliminate the definitions of SCI, Management System and Management Modules and recommend:

-
    - **Cyber Asset (CA):** Programmable electronic devices, including the hardware, software, and data in those devices. This includes platforms operating virtual machines, which are logical instances of an operating system or firmware hosted on a physical platform.
    - **EACMS:** 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 the Cyber Assets that can create, modify, delete or turn off the above Cyber Assets.
    - **PACS:** 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 the Cyber Assets that can create, modify, delete or turn off the above Cyber Assets.

SDT INTENT - Clarity is needed regarding the modifications to definitions of ERC, IRA, IS, PCA, and the retirement of ESP and EAP.

-
    i. If the SDT intended to include non-ESP ERC, modifications to existing ERC definition should include ESP and non-ESP ERC to make it compatible with the existing requirements.

    ii. If the SDT intended to include non-routable IRA access, a minor modification to the existing IRA can achieve the goal. Actually the current IRA definition has already covered the serially connected devices outside of ESP resulting from (1) the current IRA definition only states the user-initiated access using a routable protocol and doesn't say all communication sessions need to be routable all the way until the end device, and (2) it doesn't say the Cyber Asset that is accessible by a remote client has to be within an ESP. For instance, when a device serially connected to a terminal server and it can be accessible by a remote client, it meets current IRA

definition, but current CIP-005-5 R2 doesn't address IRA definition since it only apply to BCS with ERC and missed the serial connected devices.

However, the current CIP-004 R5.1 has implied an IRA definition (for terminations) applies to non-routable EACMS and PACS, where CIP-004 R5.1 requires entities to revoke IRA access to high and medium impact BCS w/ERC and associated EACMS and PACS, it implies EACMS or PACS may have IRA access even though they may not within an ESP- meaning not routable – but you have to revoke the IRA access to them. We suggest changes to IRA to make it clear that the initial access using routable protocol is one of the IRA qualifiers, where the rest of the remote access session can be non-routable.

iii. Given the proposed modifications to EACMS listed in this document, the current IS definition could remain unchanged.

iv. Definition of ESP and EAP should not be retired since they are still an effective approach for the network perimeter level security controls for physical and virtual machines. Logical isolation is not a defined term is very subjective. If the SDT intended to allow Cyber Asset level security controls, such as using local policies based firewalls, it should be an alternative measure rather than eliminating ESP and EAP approach.

v. If the SDT intended to include non-ESP PCAs, our proposed modifications to PCA can meet SDT's goal.

RECOMMENDATIONS - Modifications to ERC, IRA, and PCA:

- **ERC:** The ability to access a BCS from a Cyber Asset that is outside of the Electronic Security Perimeter in which the BCS resides via a bi-directional routable protocol connection, or the ability to access a BCS that is not within any ESPs from a Cyber Asset through an EACMS controlling communications to and from the BCS via a bi-directional routable protocol connection.

- **IRA:** User-initiated interactive access by a person employing a remote access client or other remote access technology. Remote access originates from a Cyber Asset, using a routable protocol, that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

- **PCA**: One or more Cyber Assets (1) that are connected to a BCS using a routable within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP; or (2) that are connected to a BCS using a routable protocol where an ESP model is not used and doesn't pass through any EACMS controlling communications to and from the BES Cyber System. The impact rating of Protected Cyber Assets is equal to the BCS it is connected to; (3) that share CPU or memory with a BCA, EACMS or PACS. The impact rating of Protected Cyber Assets is equal to the above highest rated Cyber Asset that shares CPU or memory with the Protected Cyber Assets.

Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	No
Document Name	

Comment

Some of the proposed changes are unclear and require clarification to correctly scope requirements. Examples include:

1. ERC – With the new definition the term “external” becomes vague. Since there would be no ESP the entity would have to define “external” to what.

2. IRA - Explanation would be needed to clearly define what a “remote access client” is in a virtual environment.

These are a few of the concerns with the proposed changes which could create a hole in applicability scoping.

Also, the retirement of well-established terms (EAP and ESP) will make entities have to make changes to their CIP program regardless if an entity moves into virtualization or not. Recommend that ESP and EAP definitions be left in the glossary of terms.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Reclamation recommends the following changes:

- Management Interface should be from within a BES level protected physical location and maintain NERC CIP electronic cyber security controls.
- Include Management Modules within the SCIdefinition..
- Include Management Interface and Modules in BCS definition.

Reclamation also identifies that Self-contained Application is essentially bundled software and may not need to be defined as a new definition within the NERC Glossary of Terms.

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

Answer	No
Document Name	

Comment

EAP and ESP should not be retired terms because they are still acceptable methods for isolating BCS from other assets and will continue to be widely used by entities that do not convert to virtualization or phase it in over time.

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 disagrees with the proposed draft definitions. The draft definitions are complex and ambiguous, which could lead to misinterpretations, improper technical implementations and increased risk of non-compliance with the NERC CIP Standards.

ISO-NE believes that the draft definitions introduce a complex and difficult matrix of possible device identifications that are theoretically mutually exclusive (Cyber Asset, Virtual Cyber Asset, Shared Cyber Infrastructure (SCI), Management Modules) and that must then be assigned one or many 'roles' (BCA, EACMS, etc.).

ISO-NE recommends that the Standard Drafting Team (SDT) create definitions that are mutually exclusive, do not embed dependencies and references to other definitions for scope, and assign only one role or categorization to a cyber system. It may be more straightforward to update the Cyber Asset definition to accommodate multiple technologies including physical or virtual components that comprise a device (such as hardware, software, and data).

Additionally, ISO-NE disagrees with the retirement of the Electronic Security Perimeters (ESP) and Electronic Access Points (EAP) defined terms. These defined terms are well understood and implemented throughout the industry with known costs and audit expectations. Retiring the ESP and EAP defined terms will require local definition of logical isolation with unknown impacts to programs as well as audit expectations. Maintaining the definitions does not prevent adoption of technology and practice that can enhance security of critical infrastructure. The SDT has publicly commented that the proposed logical isolation requirements allow for backwards compatibility and that an Entity may continue to implement ESPs and EAPs as a form of logical isolation. Therefore, these terms should not be retired and should remain active in the Glossary of Terms Used in NERC Reliability Standards.

The SCI definition seems to address specific scenarios involving storage and/or host virtualization infrastructure, but may be interpreted more broadly to include sets of systems supporting configuration management and monitoring/remediation support systems that may not have been intended for inclusion, e.g. Ansible Tower, Tripwire, and Tenable Security Center. The SDT should consider greater specification of the characteristics of "Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure."

The proposed Self-Contained Application (SCA) definition includes terms such as "isolated," which could be interpreted by Regional Entities to mean that SCAs would not be allowed network connectivity. Most containers inherently need a network address to perform their purpose.

In addition, the use of "immutable" may be problematic. The definition of Self-Contained Applications containing the term "immutable" does not apply to Containers. A running container can be configured to be 'mutable' during the runtime. This may negate containers from the definition. ISO-NE recommends revising the definition to the following suggested language:

"Packaged software, consisting of binaries that cannot be modified, containing application software, operating system, and all relevant dependencies designed to execute independent of any other software or containers residing on the same infrastructure. Self-Contained Applications may exist on Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructures."	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
We have numerous reasons for voting NO. Several other Entitys' comments show some of our concerns. After a couple years of Industry and Drafting team laborous discussions and outreach, NERC recent decided to withdrawn CIP-002-6 for FERC's approval and comments. This is a clear sign a Master Plan needs to be created instead of the current numerous different CIP Projects being run with different drafting teams. Too many old and out dated tasks and orders. Soon, and to confuse things more, there will be four CIP drafting teams all changing CIP standards, in most cases the same ones with all different implementation plans. Very confusing, expensive, and administratively budensome for registered entities. We suggest NERC work with Industry, DOE, and FERC to decide which way to procede with all CIP Standards (develop a Master Plan). Instead of having numerous drafting teams, such as this ones, working on old outdated assignments that will be changed or withrawn in the near future. It seems we are spinning our wheels and getting bogged down in paperwork and cost with no measurable/tangible reliability benefits being realized.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company supports most but not all of the proposed additions, revisions, and retirements of terms. Southern respectfully would like to make the following suggestions for SDT consideration: 1. **Electronic Security Perimeter (ESP)** – Southern requests that the definition of ESP not be retired because the transition (or no transition at all) to virtualization and/or virtualized networks will take considerable amounts of time and effort, and ESPs are still a viable form of logical isolation that can help entities and auditors if it remains active as a defined term. Southern also suggests either referring to ESP's within a new proposed definition of Logical Isolation, or adding it to the Measures as an example compliance method.	

2. **Electronic Access Point (EAP)** – Southern requests that the definition of EAP not be retired because the transition (or no transition at all) to virtualization and/or virtualized networks will take considerable amounts of time and effort, and EAPs are still a viable form of logical isolation that can help entities and auditors if it remains active as a defined term. Southern also suggests either referring to EAP's within a new proposed definition of Logical Isolation, or adding it to the Measures as an example compliance method.

a. Now, taking a step back, Southern request the SDT to also consider:

i. What if the SDT were to retire just the EAP term and then redefine ESP (keep the term) so that it can incorporate a FW on a network edge or a full ZTA "dynamic, encrypted, authenticated, and authorized session" between two objects defined in an access policy without regard to network locations? In other words, static or dynamic "perimeters". Keep the term, just define it at a more objective level than "logical border around a network" and in terms of protecting access to and from a group of applicable assets.

3. **Electronic Access Control and Monitoring System** – Southern requests that the SDT consider that the proposed modifications to the EACMS definition appears to exclude electronic access monitoring by an EACMS of the BES Cyber Systems themselves, but rather that only electronic access monitoring of the logical isolation of those systems is required.

a. Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of ***the logical isolation of BES Cyber Systems.*** *This includes Intermediate Systems.*

b. Consider this as an alternative to the EACMS definition: *Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform (1) electronic access control (including Intermediate Systems) or (2) electronic access monitoring of high and medium impact BES Cyber Systems and their associated* ***logical isolation configuration(s)****.*

4. **Logical Isolation** (Undefined Term) – Southern supports the SDT's move toward the use of the term "logical isolation", however, due to its expansive use within CIP definitions and enforceable Reliability Standards, a common understanding and definition of this term is needed to support entity compliance. Southern provides the below suggested language for consideration in this newly defined term:

a. **Logical Isolation:** the implementation of tools, devices, systems, or rules to restrict access and communications to that which is deemed necessary, and deny all other access or communications by default. Examples of Logical Isolation include the implementation of ESPs, EAPs, Zero Trust architectures, affinity rules, etc.

NOTE: *Cyber Security Incident; Electronic Access Control or Monitoring Systems (EACMS); Interactive Remote Access (IRA); Protected Cyber Asset (PCA); Removeable Media; Reportable Cyber Security Incident; Transient Cyber Asset (TCA) are all definitions that require a common understanding of "logical isolation" for it to be correctly implemented.*

5. **Cyber Security Incident** – Southern respectfully requests the SDT consider the following edits to the proposed changes to the CSI definition:

a. A malicious act or suspicious event that:

• For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) a BCS, (2) a Cyber Asset, VCA, or SCI performing logical isolation of a BCS (e.g., EACMS, SCI), or (3) a Physical Security Perimeter; or

• Disrupts or attempts to disrupt the operation of a BES Cyber System

6. **Cyber System** (Undefined Term) – Modifications have been made under the exemptions section in CIP-002-7 which move from a Cyber Asset focus to a "cyber system" focus without a corresponding definition of what that term encompasses. With the difficulty of understanding the scope of this undefined term in virtualized environments, Southern recommends developing a definition for "cyber system", such as:

a. **Cyber System:** one or more Cyber Assets, VCAs, or SCI used to perform or achieve a cyber-based objective by a Responsible Entity or other party.

b. Additionally, Southern requests the SDT to consider that Part 4.2.3.3. should be a sub-set of Part 4.2.3.2. rather than a stand alone item.

7. **Self-Contained Application** - Southern does not support the proposed definition for Self-Contained Application as it is highly technical and ambiguous in nature. Southern requests that the SDT consider the NIST defined term for "Container" below, which we believe is a clearer and more understandable definition for what Self-Contained Application is trying to achieve.

A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.

Alternatively, consider having no definition for Self-Contained Application and allow CIP-010 R1 to track changes to "application container repositories." Include in the TR or IG, entities should treat "containers/repositories" like applications and not like Cyber Assets or Virtual Cyber Assets.

8. **Shared Cyber Infrastructure** – Southern does not support the current definition of Shared Cyber Infrastructure for the following reasons:

a. The SCI definition refers to Management Systems used to initialize, deploy, ***OR*** configure, but the definition of Management Systems states that in order to be a Management System it must initialize, deploy ***AND*** configure. The two definitions appear to conflict with each other, and Southern requests that both terms use the ***AND*** conjunction.

b. **Below is a proposed revision:**

i. One or more programmable electronic devices (excluding Management Modules) and their software that share CPU, memory, or storage resources with one or more BES Cyber Systems or their associated EACMS, PACS, or PCA; this includes Management Systems used to initialize, deploy, **and** configure the Shared Cyber Infrastructure.

c. Given the complexity of trying to mix requirements that apply equally to physical Cyber Assets and Cyber Assets hosted on SCI, Southern also requests the SDT consider the possibility of splitting definitions and applicable requirements out further to avoid confusion and still provide forward-looking, objective-based requirements for each scenario. For example – the "V" prefix used below could be a qualifying indicator of "virtual" BCS, EACMS, or PACS.

i. Shared BCS Infrastructure (SBI): For H/M impact V-BCS and associated PCA.

ii. Shared Cyber System Infrastructure (SCI): For V-EACMS, or V-PACS associated with H/M BCS or SBI.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The concept of logical isolation should be defined and added to the glossary of terms. Without defining the concept of logical isolation it will lead to diverse definitions between Entities and Regions.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

During the Feb. 23, 2021 webinar, the SDT pointed out the scope of changes is limited by the SAR (V5 TAG, Order 822). When asked during the webinar, they referenced looking to the Applicable Systems where they tried to keep the proposed changes only to address those items in scope. This can be seen in numerous requirements where Management Modules only “of SCI” have been added when logically the definitions could also apply to Management Modules of any applicable stand-alone system. The SDT explained the definitions are not intended to reach outside of virtualization by bringing in patching or other configuration management systems. This is supported by the rationale presented with the proposed definitions for Management Modules and Management Systems. The proposed definitions for these glossary terms do not align with that limitation.

The Management Modules definition as written clearly includes physical Cyber Assets with out-of-band management ports, which does not align with the SDT intent discussed above.

The Management Systems definition as written would include a Cyber Asset that maintains the integrity of another Cyber Asset, through control of the processes for configuring those assets, which would expand the scope of the definition beyond virtualization.

These inconsistencies between the definitions and intended scope will inevitably cause confusion for industry and auditors. Although the expanded scope of these terms is in the best interest of Cyber Security, the definitions should be revised to match the rationale and only target the intended virtualization scope. The definitions can always be expanded in future Standards Authorization Requests when the scope of change also allows for the SDT to include the applicable stand-alone systems.

Recommendations:

Revise the definitions of Management Modules and Management Systems to limit the scope for purposes of virtualization. Suggested revisions are below.

Management Module - An autonomous subsystem of a [**delete: Cyber Asset or**] Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.

Management Systems - Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of [**delete: Cyber Assets or]** Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

Revise the definition of Shared Cyber Infrastructure to be consistent with the definition of Management Systems. Suggested revision below.

Shared Cyber Infrastructure (SCI) - One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, **[delete: or]** and configure the Shared Cyber Infrastructure.

We propose to keep the **EAP** and **ESP** as NERC Glossary terms; this will avoid future auditor interpretation issues, allow consistent application of the concepts across industry and preserve backwards compatibility.

We propose the SDT creates a glossary term for “logical isolation” to assist entities and auditors in establishing the scope of this concept as it applies to the CIP Standards.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

The IRA definition shall be review to precise the kind of access that is to be consider IRA. The actual definition doesn’t make a distinction between the engineering access and the access for issuing commands for an operator

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	
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	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
During the Feb. 23, 2021 webinar, the SDT pointed out the scope of changes is limited by the SAR (V5 TAG, Order 822). When asked during the webinar, they referenced looking to the Applicable Systems where they tried to keep the proposed changes only to address those items in scope. This can be seen in numerous requirements where Management Modules only “of SCI” have been added when logically the definitions could also apply to Management Modules of any applicable stand-alone system. The SDT explained the definitions are not intended to reach outside of virtualization by bringing in patching or other configuration management systems. This is supported by the rationale presented with the proposed definitions for Management Modules and Management Systems. The proposed definitions for these glossary terms do not align with that limitation.	

The Management Modules definition as written clearly includes physical Cyber Assets with out-of-band management ports, which does not align with the SDT intent discussed above.

The Management Systems definition as written would include a Cyber Asset that maintains the integrity of another Cyber Asset through control of the processes for configuring those assets, which would expand the scope of the definition beyond virtualization.

These inconsistencies between the definitions and intended scope will inevitably cause confusion for industry and auditors. Although the expanded scope of these terms is in the best interest of Cyber Security, the definitions should be revised to match the rationale and only target the intended virtualization scope. The definitions can always be expanded in future Standards Authorization Requests when the scope of change also allows for the SDT to include the applicable stand-alone systems.

Recommendations:

Revise the definitions of Management Modules and Management Systems to limit the scope for purposes of virtualization. Suggested revisions are below.

Management Module - An autonomous subsystem of a [delete: Cyber Asset or] Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.

Management Systems - Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of [delete: Cyber Assets or] Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

Revise the definition of Shared Cyber Infrastructure to be consistent with the definition of Management Systems. Suggested revision below.

Shared Cyber Infrastructure (SCI) - One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, [delete: or] and configure the Shared Cyber Infrastructure.

We propose to keep the **EAP** and **ESP** as NERC Glossary terms; this will avoid future auditor interpretation issues, allow consistent application of the concepts across industry and preserves backward compatibility.

We propose the SDT creates a glossary term for “logical isolation” to assist entities and auditors in establishing the scope of this concept as it applies to the CIP Standards.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CHPD has a concern with the change to the definition of EACMS. The new definition reads, “Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring **of the logical isolation of BES Cyber Systems.** This includes Intermediate Systems.” Previously, the definition stated, “… monitoring **of the Electronic Security Perimeter or BES Cyber Systems**”. The new language excludes devices that perform access control and monitoring of BES Cyber Systems. This will exclude things like AD Controllers, logging servers, etc.

Another concern is the definition of Protected Cyber Asset. CHPD had hoped that the new standards would allow more use of virtualization by clarifying the requirements and making it easier to virtualize a BES Cyber System. Instead, with the phrase “Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure” in the definition of Protected Cyber Asset it becomes too onerous to even consider virtualizing a BES Cyber System, as simply locating it on the same hardware as a non-BES Cyber System forces all the other VMs to become PCAs. Virtualization of a BES Cyber System was never impossible under the old standards, it was simply the guidance that all VMs would become PCAs that made it untenable, especially for smaller entities who do not have enough BES Cyber Systems to justify separate hardware just for them. It also does not consider network architectures that would mitigate vulnerabilities, such as isolating the virtual cluster from the internet or even the corporate network. The CPU/memory isolation language used in this definition and in other requirements make this draft untenable. Please see question 19 for more on this.

The term “asset” in the definition of IRA is not a defined term and needs to be made clearer. Either “the asset described in CIP-002 Attachment 1” or PSP could be alternatives.

One last concern is the way that scoping has been removed from the definitions. While CHPD could support the removal of scoping from the requirements, it has left the requirement language cumbersome and confusing. Scoping should be kept out of the requirement language and should be limited to the Applicable Systems language, or if that is impossible, left in the definition. For details on this, see comments on CIP-005 R1.2 in question 3.

Likes 0	
Dislikes 0	

Response

Victoria Mordi - Entergy - 3,7,9 - SERC

Answer	No
Document Name	

Comment

In reviewing the redline, there is a reference to “Internet IP” – please clarify

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1

Answer	No
Document Name	

Comment

BC Hydro SME team appreciates the opportunity to review the proposed changes and offers specific comments on the following new terms or modified definitions:

- IRA (Interactive Remote Access): The new definition of IRA no longer limits the applicability to routable protocols only. This may result in some additional communication types to be included in scope like serial over dial-up and potentially could have significant scope impact on BC Hydro's NERC CIP compliance program e.g., this removal of routable only restriction specifically affects Medium Impact BES Cyber BCS with Interactive Remote Access (IRA) and their associated PCA (CIP-005-8 R2.1) and a large number of Medium Impact BES Cyber BCS without External Routable Connectivity assets will come in scope due to this change and expansion in scope to meet the requirement of utilizing an Intermediate System as per the new definition of IRA.

Secondly, we seek clarity on the terms used in the definition of IRA e.g., what is the difference between outside of the asset containing the system being accessed (what is defined as the 'asset') vs. outside of the logical isolation. A typical example is an asset that could be a transmission station or a specific line. If a digital protection relay associated with line has a logical isolation perimeter, would there be concerns with communications from within the station but outside that perimeter, or only with communications from outside of the station completely, as stated in the IRA definition with the specific use of the 'OR' condition.

BC Hydro recommends that the definition of the IRA continues to include the use of the terms related to routing, and suggests that IRA be defined as follows:

"User-initiated access by a person employing a remote access client from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed, or other remote access technology using a routable protocol."

SCA (Self-Contained Application): We request additional clarification and/or examples on SCA, e.g. examples of immutable software in NERC CIP environment.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Request clarification of Logical Isolation definition. Is the intended definition “The logical border surrounding a VCA associated to a BES Cyber Systems which is connected using a routable protocol”?

Request the review of the EACMS definition or define logical isolation, because the current definition is suggesting that only EACMS are to be used for logical isolation which is not the current case. For example, the usage of an Active Directory could be associated to a BES Cyber System only and not to a logical isolation. Suggest reinstating the “OR”, of the logical isolation Electronic Security Perimeter(s) of BES Cyber Systems or BES Cyber Systems.

Request the review of the Shared Cyber Infrastructure (SCI), the definition seems to define two types of objects; the first object being the server that is sharing the CPU, memory, or storage and the second oject is the console (management system) which is used to initialize, deploy, or configure the Shared Cyber Infrastructure. So in the VMWARE world, the ESX is SCI and the VCenter is a SCI.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6

Answer	No
Document Name	

Comment
Oklahoma Gas and Electric supports the comments provided by EEI.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx

Comment
See attachment for comments.

Likes 0	
Dislikes 0	

Response

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	

Comment
Basin Electric's concern is that it appears that none of this is applicable to the cloud throughout this project 2016-02 and none of it identifies it as such. This hinders NERC's ability to move forward in the area of cloud based applications. Again - this applies across the board to all questions. Are they going to keep the concept of EAC and EAMs? Basin would be in support of this depending on how they define and write up EAC and EACMS.

Storage array issue - since storage array wasn't directly impacting assets, this would massively impact Basin Electric - goes against how we have been defining that. PACS on to the storage array - which by these new definitions, the implication would be that we would need separate storage array for assets that are in scope. Inherent separations are there such as encryption, so this would cause quite a bit of additional work here. NERC needs to clearly identify what is contained here.

Section D - logical isolation is not a defined term. We would like to see an actual definition for "logical isolation"

IRA recommendation - would rope in all desktops by definition to Cyber Assets but not BES Cyber Assets. Clarify between BES Cyber Asset - BROS reliability impacts - 15 minute impact; Cyber Asset is all encompassing, programmable electronic devices that include hardware, software.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) suggests that the phrase, “or other remote access technology” does not need to be removed from the Interactive Remote Access definition. The proposed definition for Interactive Remote Access (IRA) seems to dictate a remote access client must be used. Otherwise, entities not using a remote access client would not consider their remote connections to be IRA.

The proposed definition for Intermediate Systems is overly broad and could potentially label other EACMS (such as Cyber Assets controlling two-factor authentication or domain controllers) as Intermediate Systems as these systems aid in restricting IRA. Furthermore, Intermediate Systems do not by themselves restrict IRA. For instance, access control for a Microsoft Windows server acting as a jump host (Intermediate System) is performed by a domain controller.

External Routable Connectivity (ERC) as previously defined using the Electronic Security Perimeter (ESP) implied a degree of separation between a system with ERC and the external world, even though it doesn’t use physical or geographical terms. The new definition removes the words “that is outside of its associated ESP” since ESP is no longer defined. This makes the definition confusing and could possibly be misinterpreted. For example, in a segmented network, each BCS could have ERC to its neighbor in the same rack if traffic is traversing a firewall or router with ACLs defined.

ERC was meant to define access from outside the asset facility, not from the same rack. It is not clear this new definition means what is intended.

CEHE suggests retaining a sense of separation by saying ERC originates from: a) a Cyber Asset not identified in CIP-002; b) an identified Cyber Asset located at another asset; or c) an identified Cyber Asset that is logically separated behind a different EACMS. These criteria may not be airtight, but begin to address this issue, where a BCS could have ERC to its physical neighbor but not to a Control Center that controls it.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Southern Indiana Gas & Electric Company d/b/a CenterPoint Energy Indiana South (SIGE) suggests that the phrase, “or other remote access technology” does not need to be removed from the Interactive Remote Access definition. The proposed definition for Interactive Remote Access (IRA) seems to dictate a remote access client must be used. Otherwise, entities not using a remote access client would not consider their remote connections to be IRA. The proposed definition for Intermediate Systems is overly broad and could potentially label other EACMS (such as Cyber Assets controlling two-factor authentication or domain controllers) as Intermediate Systems as these systems aid in restricting IRA. Furthermore, Intermediate Systems do not by themselves restrict IRA. For instance, access control for a Microsoft Windows server acting as a jump host (Intermediate System) is performed by a domain controller. External Routable Connectivity (ERC) as previously defined using the Electronic Security Perimeter (ESP) implied a degree of separation between a system with ERC and the external world, even though it doesn’t use physical or geographical terms. The new definition removes the words “that is outside of its associated ESP” since ESP is no longer defined. This makes the definition confusing and could possibly be misinterpreted. For example, in a segmented network, each BCS could have ERC to its neighbor in the same rack if traffic is traversing a firewall or router with ACLs defined. ERC was meant to define access from outside the asset facility, not from the same rack. It is not clear this new definition means what is intended. SIGE suggests retaining a sense of separation by saying ERC originates from: a) a Cyber Asset not identified in CIP-002; b) an identified Cyber Asset located at another asset; or c) an identified Cyber Asset that is logically separated behind a different EACMS. These criteria may not be airtight, but begin to address this issue, where a BCS could have ERC to its physical neighbor but not to a Control Center that controls it.	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

IRA—The changes to Interactive remote Access (IRA) could use some additional changes. The phrase “outside of the asset containing the system being accessed” seems like it could be removed. Many entities use logical isolation to control access to groups of assets (whether virtual or physical) within the current ESP definition. There shouldn’t be a requirement to control access from each device but simply a requirement to show that there are controls in place to prevent access. This can be done by showing logical or physical isolation, which would include an asset or group of assets. The remaining phrase “from outside of the logical isolation of the system being accessed” appears sufficient to meet this intent.

PCA —The changes to the Protected Cyber Asset (PCA) definition has a phrase that states “that are being actively remediated prior to indroduction to the production environment.” This seems to indicate a compliance activity or compliance requirement and not a compliance definition. It is not clear from this phrase what is being actively remediated. The rationale indicates that it is while the VCA is being prepped from deployment, but there still appears to be a lack of clarity with mixing definitions and activities and this could use some clean up. Additionally, in the previous defintions, PCA was defined as something that was routably connected to a BCS. This newly proposed definition moves to a concept of logically isolated. It is unclear at this time what is expected to logically isolated a devices from a BCS when the devices is serially connected to the BCS. Therefore, it makes it makes it unclear if a device qualifies as a PCA when it is serially connected to a BCS with this proposed definition.

Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	
Response	

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

AZPS agrees with the comments provided by EEI on the proposed additions, revisions, and retirements of terms. A further clarification to the following definitions would be appreciated:

1. Logical Isolation (Undefined Term) – AZPS recommends “logical isolation” be defined. A clear understanding of this term is necessary given that new and revised CIP definitions rely on this term. Additionally, a definition is needed to support compliance.

2. Cyber System (Undefined Term) - AZPS recommends developing a definition for “cyber system”. The exemptions contained within CIP-002-7 have moved from a Cyber Asset focus to one that focuses on the undefined term “cyber system”. The development of a definition for cyber system is needed to provide a common understanding for compliance.

3. Cyber Security Incident; Electronic Access Control or Monitoring Systems (EACMS); Interactive Remote Access (IRA); Protected Cyber Asset (PCA); Removeable Media; Reportable Cyber Security Incident; Transient Cyber Asset (TCA) – AZPS generally supports the revisions of these terms, however, the definitions for these terms rest on a common understanding of “logical isolation”. Logical isolation should be defined prior to implementing these changes.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP agrees with many of the proposed additions, revisions, and retirements of terms. While we support modifications to the CIP Reliability Standards and associated definitions that more clearly accommodate virtualization, it is imperative that legacy solutions remain in the standards for those entities who intend to continue to use those solutions.

AEP generally supports EEI’s suggestions and further suggests that acceptable methods of Logical Isolation including ESP, Zero Trust, etc. should be included in the definition of Logical Isolation and not include these acceptable methods within Measures. These suggestions are listed below.

Electronic Security Perimeter (ESP) – AEP does not support the retirement of this term because some companies may not have immediate plans or ability to move to virtualized networks. While we support changes made to CIP-005, the retirement of the term ESP without some reference to this term within the definition of logical isolation or within the measures within CIP-005 could create confusion. To resolve this concern, AEP requests the term ESP to be referenced within the definition of logical isolation.

Electronic Access Point (EAP) – AEP does not support the retirement of this term because many companies may not have immediate plans or ability to move to virtualized networks. AEP requests similar accommodations as suggested above within our comments regarding ESPs.

Logical Isolation (Undefined Term) – AEP supports the move toward the use of the concept of “logical isolation,” however, due to its expansive use within the Reliability Standards, a definition of this term is needed. In developing a definition, AEP requests that the definition for logical isolation include ESP as an acceptable method of Logical Isolation within a defined term. NOTE: *Cyber Security Incident; Electronic Access Control or Monitoring*

Systems (EACMS); Interactive Remote Access (IRA); Protected Cyber Asset (PCA); Removable Media; Reportable Cyber Security Incident; Transient Cyber Asset (TCA) are all definitions that require a common understanding of "logical isolation" to be fully understood.

Cyber System (Undefined Term) - AEP recommends developing a definition for "cyber system" as a defined term. The Exemptions section contained within all of the proposed CIP Reliability Standards have moved from a Cyber Asset focus to one that focuses on the undefined term "cyber system". The development of a definition for cyber system is needed to provide a common understanding for compliance.

Self-Contained Application - AEP does not support the proposed new definition for Self-Contained Application and questions the need for this term. AEP recommends commonly used and understood IT terms be used. In place of the proposed term, AEP suggests the IT term "Container", which is commonly understood and appears to have the same definition as proposed for "Self-Contained Application".

Shared Cyber Infrastructure (SCI) – AEP does not support the currently proposed definition for Shared Cyber Infrastructure for the following reasons:

- The proposed definition refers to Management Systems used to initialize, deploy, **OR** configure but the definition of Management Systems states that to be a Management System it must initialize, deploy, **AND** configure. These two definitions presently conflict with each other. Before the proposed definition of SCI can be accepted, the identified conflict between this term and its companion term (Management Systems) needs to be harmonized.
- Currently, the scope of SCI is unclear. An explanation of the limiting factors for the scope of SCI regarding their software should be provided, e.g., would the firmware of a server blade be included within the scope of SCI?
- AEP also suggests that the proposed definition would be more easily understood if more language and terms were drawn from current NERC CIP acronyms rather than using their long form names.
- The term SCI may not be clear or fully understood by all entities and we suggest adding examples within the Technical Rationale.

Interactive Remote Access (IRA): While AEP understands the need to streamline the definition of IRA, additional clarification is needed to better describe IRA in the context of virtualization, particularly regarding serial links.

Management Systems: This definition appears to align with the definition of a hypervisor, however, it also includes some language that tries to straddle between both virtualized and non-virtualized environment. This ambiguity may create confusion, and AEP recommends the definition be clarified. It may also be helpful to include some examples of Management Systems within the Technical Rationale.

External Routable Connectivity (ERC): AEP recommends adding "or SCI" at the end of the proposed modification once the definition of SCI is clarified. Current draft reads, "The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset through an Electronic Access Control or Monitoring System controlling communications to and from the BES Cyber System that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection."

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

AEPCO is signing on to ACES comments, see below:

ACES feels it's time to address Intermediate Systems (IS) as applicable systems without lumping it in with EACMS. This will allow for more granular controls for IS without having to change other standards and requirements.

On the NERC/SDT webinar, the term "Self-Contained Application" wasn't covered thoroughly. The term is only used in CIP-010, and the definition seems to allude to a software appliance/package such as a virtual firewall, router, etc. Further, if software is running in a truly isolated environment the only security risk would be a physical attack. ACES does not see the need for this Term.

External Routable Connectivity's definition does not read well. Having Cyber Asset or Virtual Cyber Asset in the definition limits scope to those asset classes. The "from" is irrelevant and should be not be limited to any type of device. The definition is founded in communication, not Cyber Assets. Proposed language: The ability to communicate, via a bi-directional routable protocol connection, with a BES Cyber System or Shared Cyber Infrastructure from outside of the BES Cyber System's or Shared Cyber Infrastructure's logical isolation.

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

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

Proposed definitions such as Management Module, Management Systems, Self-Contained Applications, Revised IRA definitions are vague or confusing. Definitions should not rely on rationale documents as a supplement; rather, they should be clear in a standalone format within NERC Glossary of Terms. There appears to be some overlap between the definition of SCI and Management Systems. As the new proposed definitions are used to determine applicability, their clarity is extremely important. We recommend further clarifications be made to these new definitions. As the new/revised definitions are the basis for all the revisions, Hydro One is not able to support the proposed revisions to CIP Standards at this time.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Multiple new terms were added to the standards in this project but not defined within the NERC Glossary of Terms. CIP-005 introduced “controlled communications”, but did not clarify what controlled communications is. Additionally, “System Hardening” was add to CIP-007, but was not defined.	
Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren generally agrees with EEI's comments with some added suggestions. We suggest that logical isolation should be fully defined, and also suggest using the term "logical border" instead of logical isolation. We suggest that assets should be required to have one logical border. In regards to the term Cyber System, Ameren suggests the definition Collection of Cyber Capable Devices. We ask that the SDT not be too prescriptive in their definition, and suggest using the NERC Glossary of terms definition. We differ with EEI's suggestion for Self-Contained Application because if there's new technology that isn't a container, it could be classified as SCA. Regarding Shared Cyber Infrastructure, Ameren suggests including examples of systems, and we ask that the scope be more defined. Regarding Interactive Remote Access, Ameren believes that the definition provided doesn't make much sense, as current remote workspaces would be considered remote access.	
Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	

Definition changes are extremely confusing and do not follow Industry standard terminologies. Many terminologies do not reference BES and hence its extremely confusing.

Furthermore, most new definitions are not required; just BCS definition is sufficient. All other elements must follow, high watermarking and security controls and standards must apply.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Definition changes are not clear and will cause confusion as well as differing interpratations.

Concerns with the definition changes creating a gap in applicable system scope. Proposed defintions appear to create multiple identifiers (SCI, EACMS, Intermediate System, PCA) to the same device.

We suggest keeping the ESP and EAP definitions in the active portion of the glossary.

Does new ERC definition introduce a new Requirement?

Other areas of concern include

- What is the definition of a “remote access client?” 2)
- Need clarification on “outside the asset”.
- Need clarification on the relationship of physical isolation to logical isolation
- Need clarification in regards to Intermediate Systems. The proposed definitions can be interpreted to include firewalls as Intermediate System.
- Need clarification on Management Module and Management Systems
- Need clarification of SCI’s definition. The proposed definition of SCI could include network devices. SCI interpretations say that network services are not SCI.
- Need clarification on Storage. Appears that Storage is a Cyber Asset but not part of a Virtual Cyber Asset. This appears inconsistent.
- Need clarification on Virtual Cyber Asset as a Protected Cyber Asset

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

Likes 0	
Dislikes 0	

Response

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

Comment
Texas RE appreciates the Standard Drafting Team's (SDT's) efforts to establish a framework to specifically address the implementation of virtualized CIP architectures within CIP environments. Nevertheless, Texas RE does not agree that wholesale changes are need to the CIP standards to address virtualization. Instead, Texas RE suggests the SDT consider creating virtualization specific terminology that is applicable to the current overarching CIP framework. Texas RE believes this is best accomplished by (1) amending current CIP definitions to specifically address virtualization concepts; and (2) creating virtualization specific definitions where appropriate. Consistent with this overarching view, Texas RE has the following comments on the proposed definitions: **Electronic Access Control or Monitoring Systems (EACMS)** Texas RE seeks clarification on why the SDT proposed to remove the phrase "or BES Cyber Systems" found in the current approved EACMS definition. Removing this language could inadvertently remove Cyber Assets such as log collectors, SIEMS, and active directories from being identified as EACMS because they do not "*perform electronic access control or electronic access monitoring of the logical isolation of BES Cyber Systems*." Texas RE instead suggests retaining the concept that EACMS include Cyber Assets that perform electronic access monitoring of either logical isolation or BES Cyber Systems to include these devices. Additionally, Texas RE strongly recommends the proposed EACMS definition retain the five EACMS functions – (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; and (5) alerting – documented in CIP-002-5.1a, recognized by the SDT in the CIP-008-6 project, and documented by FERC addressing enhanced reporting for EACMS performing those five functions. This inclusion will reduce ambiguity by clarifying the functional attributes associated with EACMS. **BES Cyber System Information (BCSI)** The words "ESP names" was removed with no replacement. Texas RE recommends adding the words "Logical Isolation names" to ensure clarity. **Electronic Access Point (EAP)**

Texas RE does not agree this term should be retired. Please see the comments regarding CIP-005 in response to the SDT's Question No. 2.

External Routable Connectivity (ERC)

The current language states "…through an Electronic Access Control or Monitoring System controlling communications...". If in the scenario, routable protocol is being used but not through an EACMS, then by definition there would be no ERC. Texas RE recommends revising the language to "*The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure that is outside its associated logical isolation via a bi-directional routable protocol connection*."

Electronic Security Perimeter (ESP)

Texas RE does not agree this term should be retired. Please see the comments regarding CIP-005 in response to SDT Question No. 2. Texas RE recommends defining "logical isolation" for clarity. The undefined term "routable protocol" should be defined to address layer 3 traffic. In part 1.5 further confusion is added by using an uppercase "Internet Protocol (IP)", which is also not defined. In Texas RE's experience, these undefined terms have caused interpretation issues in the past. Texas RE therefore recommends limited use of undefined terms in the proposed Standard Requirement revisions.

Interactive Remote Access (IRA)

Removing the words "or other remote access technology", causes a risk that if a remote access client is not used then it is out of scope for IRA. To address this and ensure a comprehensive IRA definition, Texas RE recommends the proposed IRA definition be revised to read: "User-initiated access by a person employing remote access technology outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed."

Intermediate Systems

Texas RE recommends the proposed Intermediate Systems definition be adjusted slightly to address the possibility that there could be one or more EACMS used to restrict IRA by adding "(s") to the EACMS definition. The revised language would read: "*Electronic Access Control or Monitoring System(s) that is used to restrict Interactive Remote Access*."

Cyber Asset

Texas RE recommends the definition of Cyber Asset be renamed to "Hardware Cyber Asset" to make the distinction with Virtual Cyber Asset.

BES Cyber Asset (BCA)

Consistent with Texas RE's suggested revisions to the "Cyber Asset" definition to better clarify the distinction between physical and virtual Cyber Assets, Texas RE further recommends that the SDT revise the BCA definition to "A Hardware Cyber Asset or Virtual Machine that" in order to clarify that BCAs include both physical and virtual Cyber Assets.

Virtual Cyber Asset (VCA)

Texas RE recommends aligning the VCA definition set forth in NIST's Computer Security Resource Center glossary as proposed below. The SDT could accomplish this by either addressing the concepts below in the VCA definition itself or creating new definitions.

New term: Virtual Machine.

Definition: A simulated environment created by Virtualization.

New term: Hypervisor.

Definition: The Virtualization component that manages the guest OSs on a Virtualized Host and controls the flow of instructions between the guest OSs and the physical hardware.

New term: Virtualized Host.

Definition: The Hardware Cyber Asset on which the virtualization software such as the Hypervisor is installed. Usually, the Virtualized Host will contain a special hardware platform that assists virtualization - specifically Instruction Set and Memory virtualization. Virtualized Hosts inherit the impact rating and categorization of all hosted Virtual Machines. This phrase would be used instead of Shared Cyber Infrastructure (SCI).

New term: Virtualization.

Definition: The simulation of the software and/or hardware upon which other software runs.

New term: Container

Definition: A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.

Shared Cyber Infrastructure (SCI)

Texas RE believes that the proposed definition for "Shared Cyber Infrastructure" is too broad in scope. Texas RE reads the current language to include devices normally considered part of the Cyber Asset definition.

Many computer systems are, by design, discrete programmable electronic devices joined together to serve a collective function. This is accomplished by sharing one or more of their CPU, memory, or storage resources with each other. For example, a video card is a programmable electronic device. It shares its CPU and resources with the Cyber Asset it is installed on. As such, it would appear to meet this definition of SCI. Along similar lines, because a data storage virtualization technology (RAID) controllers share their storage resources with the Cyber Assets in which they are installed, such storage technology controllers would also appear to meet this definition. Finally, a computer's motherboard is a programmable electronic device. Its primary function is to facilitate the sharing of CPU, memory, and storage resources between the various discrete devices that have been connected to it. Texas RE respectfully requests the SDT consider these examples in developing an appropriate SCI definition.

Management Modules

Texas RE recommends defining the phrase “autonomous subsystem” as the definition of Management Modules may pull into scope certain devices, depending on how “autonomous subsystem” is defined. For example, some data storage virtualization technology (RAID) controllers provide management and monitoring capability independent of the host system’s CPU, firmware, or operating system. As such, these data storage virtualization technology controllers would appear to meet the definition of Management Module.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

IESO supports TFSIT/NPCC comments.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	

Comment

The definition of Shared Cyber Infrastructure is open to multiple interpretations as written. The confusion is compounded by the exclusion of Shared Cyber Asset from the definition of Cyber Asset (Cyber Asset itself a problematic definition at times). The intent of the SDT is unclear preventing recommending an alternative proposal.

The definition of Intermediate System is excessively hazy and could be interpreted to mean an authentication system or a Jump host. The intent of the SDT is unclear preventing recommending an alternative proposal.

NERC, including the SDT, needs to be prepared and ensure that adequate CMEP SDT developed guidance is in place to broadly communicate the intent, implementation guidance, and interpretation of the new definitions on passage and prior to NERC Membership and our vendors beginning work to bring systems into compliance. In general terms, WVPA would have preferred that the SDT adopted the terms and directly adapted the definitions used by NIST in their documentation, such as NIST SP 800-125.

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 it's time to address Intermediate Systems (IS) as applicable systems without lumping it in with EACMS. This will allow for more granular controls for IS without having to change other standards and requirements. On the NERC/SDT webinar, the term "Self-Contained Application" wasn't covered thoroughly. The term is only used in CIP-010, and the definition seems to allude to a software appliance/package such as a virtual firewall, router, etc. Further, if software is running in a truly isolated environment the only security risk would be a physical attack. ACES does not see the need for this Term. External Routable Connectivity's definition does not read well. Having Cyber Asset or Virtual Cyber Asset in the definition limits scope to those asset classes. The "from" is irrelevant and should be not be limited to any type of device. The definition is founded in communication, not Cyber Assets. Proposed language: The ability to communicate, via a bi-directional routable protocol connection, with a BES Cyber System or Shared Cyber Infrastructure from outside of the BES Cyber System's or Shared Cyber Infrastructure's logical isolation.	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports the response submitted by TVA.	
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	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

Concerns on the definitions may result in a no vote in standards that use those definitions.

Cyber Asset: The current term is “Assets”. The proposed term is “Asset”. The language in the definition is still plural. Solution to make it singular.

Electronic Access Control or Monitoring Systems (EACMS): SDT members have said that VLANS are not allowed because network equipment is not considered SCI since “network services” are not included in what the SCI is sharing. If this is the case, it is difficult to understand why SCI is included in the proposed definition of EACMS.

Need clarification: Is the logical isolation of a Cyber Asset(ie. Windows based firewall) that is part of a system (BCS, Intermediate Systems...) the same as logical isolation of the system? It seems that the Windows based firewall that may be implemented on a Intermediate System or BES Cyber Asset could be considered an EACMS. If this is true then all communication to that Cyber Asset would be ERC.

Electronic Access Point: In order to maintain backward compatibility, this term should not be retired. It has been mentioned that retired terms would be retained in the “Retired Terms” section of the NERC Glossary and therefore not need to be defined by each entity that wishes to use these terms in their compliance documents. It is our view that retired terms and their definitions are no longer recognized by NERC and therefore would have to be redefined by each entity.

Electronic Security Perimeter: This term, or something that captures a boundry between what is protected and what is not protected need to be retained in order to make the “External” in ERC have meaning.

In order to maintain backward compatibility, this term should not be retired In order to maintain backward compatibility, this term should not be retired. It has been mentioned that retired terms would be retained in the “Retired Terms” section of the NERC Glossary and therefore not need to be defined by each entity that wishes to use these terms in their compliance documents. It is our view that retired terms and their definitions are no longer recognized by NERC and therefore would have to be redefined by each entity.

External Routable Connectivity (ERC): The ERC definition used “Electronic Access Control or Monitoring System controlling communications to and from the BES Cyber System”. The Intermediate System definition uses “An Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access.” It is unclear what the difference is between “controlling” and “restricting”. Solution consistency in language regarding the concept(s).

The proposed definition would make any controlled communication ERC even if that communication is within what would have been the ESP. For examples, an ESP with an internal VLAN would now have ERC for communication between VLANS, communication through a Windows based firewall on a BCA or Intermediate System would be ERC.

Interactive Remote Access (IRA): Does "asset" mean the CIP-002 R1 assets?

Because the network equipment is not clearly excluded from being SCI based on the SCI definition, VLANs could be allowed as logical isolation. Defense in Depth strategies would also create logic isolation within a BCS. Both of these situations could cause IRA to be used for communication performed inside the what was an ESP.

Request clarification on the difference or relationship between physical and logical isolation. The definitions and standards only list logical isolation.

Intermediate Systems: A firewall would implicitly or explicitly restrict Interactive Remote Access that was attempted through it. Therefore, a firewall would be an Intermediate System. This is not consistent with how the term is used in the CIP standards and the security controls that the Intermediate System is intended to provide. Did you intend this definition to be this broad? Example: A router could be Intermediate System based upon the language. Please clarify the intent of this definition.

The term was changed from “System” to “Systems” but the language is still singular.

Management Interface: A Protection System Relay control panel or on/off button may meet this definition. Define monitor. Is a local display, monitoring? Does monitoring require alarms? What do you mean by a physical interface? Why define a term that is only used once in CIP-005-8 R1.2? Suggest that definitions only used in a single requirement should not be defined in the NERC glossary. This would be consistent with the removal of the LERC and LEAP terms.

Is monitoring, as it is used here, consistent with the use in PRC-005?

Management Module: Based on discussions with SDT members, the definition of this term may be based on how it is used in the standards. We believe that all definitions should be clearly written and understood, independent of their use in the standard.

Is it correct that the panel on a Protection System Relay is not a MM because it is not independent of the host systems….?

Does Wake on LAN meet this definition?

Is the Management Module part of the Cyber Asset or is it a separate Cyber Asset? It seems that an autonomous subsystem could be identified as a Cyber Asset.

Please provide some examples of these devices.

Management Systems: Is the use of integrity consistent with its use in CIP-010-5 R1.4? What is the "those assets and systems" referencing at the end? Should it be “Cyber Assets and BCS? Solution “systems” should be removed and “assets” replaced with Cyber Assets and Virtual Cyber Assets.

The Technical Rational restricts this definition to virtual environments but the definition does not include this restriction. It seems that tools such as Ghost, used to image systems, might meet this definition.

Removable Media: What does it mean to be "directly connected .. to .. a network". If thumb drive is connected to a USB port of a PCA but that drive is not shared as a network device, was it connect to the network? What is the difference between "a network not logically isolated from…" and a PCA? Was it the intent of the SDT to remove directly connecting to a PCA?

If I had two BCS each on its own VLAN that all PCA's would be isolated from the other "logical network (VLAN)" and not be Removeable Media if plugged into PCA.

Suggest formatting the proposed Removeable Media definition in the same way that the TCA definition is formatted.

Self-Contained Application: This is only used in CIP-010 R1.1.1 and R1.1.2 for change authorization. Suggest that definitions only used in a single requirement should not be defined in the NERC glossary. This would be consistent with the removal of the LERC and LEAP terms.

Shared Cyber Infrastructure (SCI): In discussions with SDT members, it was stated that VLANs are not allowed because the proposed SCI definition does not include the sharing of "network services". Some network devices would meet the proposed definition of SCI. The fact that other aspects of these network devices are not listed in the definition does not exclude them from meeting the definition. The proposed definition of SCI must be modified to clearly remove network devices if this is the intent of the SDT.

Transient Cyber Asset (TCA): Not logically isolated would include devices that are physically isolated. Solution clarify the difference between physical and logical isolation.

Need a better understanding of how a VM that spawns for a short period of time is treated. Is the VM image (or whatever it is called) the VCA and not the image or images that are spawned.

The following terms are used but not defined by the SDT.

Logical Isolation: Would like this term defined to include the relationship with physical isolation.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

Southwest Power Pool (SPP) offers the following comments and questions for the SDT consideration of Question 1:

Cyber Asset Definition - The definition of a Cyber Asset is confusing with the exclusion of SCI.

EAP Definition – Consideration that if there is a retirement of EAP, and if we keep with backwards compatibility while using an ESP, we will still need the EAP definition.

ERC Definition - The definition of ERC is confusing because of the introduction of logical isolation. What happens to the IAL network?

IRA Definition - Based on the new definition of IRA, every time you connect to a CIP asset in the same logical isolation area, you are doing ERC. This is not the case in the current version of the standard, and adds a level of confusion.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for the definitions. PG&E does have concerns and supports the input provided by EEI.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

During the Feb. 23, 2021 webinar, the SDT pointed out the scope of changes is limited by the SAR (V5 TAG, Order 822). When asked during the webinar, they referenced looking to the Applicable Systems where they tried to keep the proposed changes only to address those items in scope. This can be seen in numerous requirements where Management Modules only “of SCI” have been added when logically the definitions could also apply to Management Modules of any applicable stand-alone system. The SDT explained the definitions are not intended to reach outside of virtualization by bringing in patching or other configuration management systems. This is supported by the rationale presented with the proposed definitions for Management Modules and Management Systems. The proposed definitions for these glossary terms do not align with that limitation.

The Management Modules definition as written clearly includes physical Cyber Assets with out-of-band management ports, which does not align with the SDT intent discussed above.

The Management Systems definition as written would include a Cyber Asset that maintains the integrity of another Cyber Asset through control of the processes for configuring those assets, which would expand the scope of the definition beyond virtualization.

These inconsistencies between the definitions and intended scope will inevitably cause confusion for industry and auditors. Although the expanded scope of these terms is in the best interest of Cyber Security, the definitions should be revised to match the rationale and only target the intended virtualization scope. The definitions can always be expanded in future Standards Authorization Requests when the scope of change also allows for the SDT to include the applicable stand-alone systems.

Recommendations:

Revise the definitions of Management Modules and Management Systems to limit the scope for purposes of virtualization. Suggested revisions are below.

Management Module - An autonomous subsystem of a [delete: Cyber Asset or] Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.

Management Systems - Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of [delete: Cyber Assets or] Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

Revise the definition of Shared Cyber Infrastructure to be consistent with the definition of Management Systems. Suggested revision below.

Shared Cyber Infrastructure (SCI) - One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, [delete: or] and configure the Shared Cyber Infrastructure.

We propose to keep the **EAP** and **ESP** as NERC Glossary terms; this will avoid future auditor interpretation issues, allow consistent application of the concepts across industry and preserves backward compatibility.

We propose the SDT creates a glossary term for “logical isolation” to assist entities and auditors in establishing the scope of this concept as it applies to the CIP Standards.

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 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

Concerns with definitions could result in NO votes.

Concerns with the definition changes creating a gap in the applicable system scope. The current definitions define scope boundaries (such as ESP, ERC, EAP, IRA) with established demarcations. It is also unclear if multiple identifiers (SCI, EACMS, Intermediate System, PCA) are applied to the same device, causing overlapping scoping requirements (it is unclear of interactions or precedence). The modification or retirement within the proposed definitions causes confusion on the interpretation and application of current and future CIP program-related decisions to remain in compliance.

Request keeping the ESP and EAP definitions in the active portion of the glossary. Having a section for retired terms will not help with compliance. We prefer a clear delineation.

Does the new ERC definition introduce a new Requirement?

ERC comments; 1) request clarification on “external” to what? 2) request clarifications on how VLANs work with ERC 3) request clarification on where the PCAs are 4) Request clarification on physical security, like air gapping, and 5) request that any definition be consistent wherever it is used instead of needing to review the intersection of each definition with each Requirement’s Applicability.

IRA comments; 1) where is the definition of a “remote access client?” 2) request clarification on “outside the asset” – is that referring to CIP-002 R1? 3) request clarification on the relationship of physical isolation to logical isolation.

Request clarification on Intermediate Systems. The proposed definitions can be interpreted to include firewalls as Intermediate System. This would remove the Intermediate Systems requirement as required now and impose additional controls on firewalls that are unnecessary.

Request clarification on Management Module and Management Systems – should the entity internally define “management and monitoring capabilities?” SCI definition use AND while the Management Systems definition uses OR. Request consistency.

Was PCA intentionally removed from the definition of Removable Media?

Request clarification of SCI’s definition. The proposed definition of SCI could include network devices. SCI interpretations say that network services are not SCI.

Request clarification on Storage. Appears that Storage is a Cyber Asset but not part of a Virtual Cyber Asset. This appears inconsistent.

Request clarification on Virtual Cyber Asset as a Protected Cyber Asset.

Request clarification of Logical Isolation definition, is the expected definition be “The logical border surrounding a VCA associated to a BES Cyber Systems which is connected using a routable protocol.

Request the review of the EACMS definition or define logical isolation, because the current definition is suggesting that only EACMS are to be used for logical isolation which no the current case. For example, the usage of an Active Directory could be associated with a BES Cyber System only and not perform logical isolation. Suggest reinstating the “OR”, of the logical isolation Electronic Security Perimeter(s) of BES Cyber Systems or BES Cyber Systems.

Request the review of the Shared Cyber Infrastructure (SCI), the definition seems to define two types of objects; the first object being the server that is sharing is CPU, memory, or storage and the second object is the console (management system) which is used to initialize, deploy, or configure the Shared Cyber Infrastructure. So, in the VMWARE world, the ESX is SCI and the VCenter is an SCI.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb 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; - Douglas Webb

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 1.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI agrees with many of the proposed additions, revisions, and retirements of terms. While we support modifications to the CIP Reliability Standards and associated definitions that more clearly accommodate virtualization, it is imperative that legacy solutions remain in the standards for those entities who intend to continue to use those solutions. It is from this perspective that EEI offers the following suggestions for consideration.

Electronic Security Perimeter (ESP) – EEI does not support the retirement of this term because some companies may not have immediate plans or ability to move to virtualized networks. While we support changes made to CIP-005, the retirement of the term ESP without some reference to this term within the definition of logical isolation or within the measures within CIP-005 could create confusion. To resolve this concern, EEI recommends the term ESP either be referenced within the definition of logical isolation or a reference to ESPs be included within CIP-005 within Measures.

Electronic Access Point (EAP) – EEI does not support the retirement of this term because many companies may not have immediate plans or ability to move to virtualized networks. EEI recommends similar accommodations as suggested above within our comments regarding ESPs.

Logical Isolation (Undefined Term) – EEI supports the move toward the use of the concept of "logical isolation," however, due to its expansive use within the proposed Reliability Standards a definition of this term is needed. In developing a definition, EEI requests that the definition or measures for logical isolation include ESP as an acceptable method of Logical Isolation. E.g., include in the measures that acceptable methods of Logical Isolation include ESP, Zero Trust, etc. NOTE: *Cyber Security Incident; Electronic Access Control or Monitoring Systems (EACMS); Interactive Remote Access (IRA); Protected Cyber Asset (PCA); Removeable Media; Reportable Cyber Security Incident; Transient Cyber Asset (TCA) are all definitions that require a common understanding of "logical isolation" to be fully understood.*

Cyber System (Undefined Term) - EEI recommends developing a definition for "cyber system". The "Exemptions" section contained within all of the proposed CIP Reliability Standards have moved from a Cyber Asset focus to one that focuses on the undefined term "cyber system". The development of a definition for cyber system is needed to provide a common understanding for compliance. (Questions about the difficulty of defining in virtualized environment.)

Self-Contained Application - EEI does not support the proposed new definition for Self-Contained Application and questions the need for this term. EEI recommends commonly used and understood IT terms be used. In place of the proposed term, EEI suggests the IT term "Container", which is commonly understood and appears to have the same definition as proposed for "Self-Contained Application". NIST defines Container as the following:

A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.

Shared Cyber Infrastructure – EEI does not support the currently proposed definition for Shared Cyber Infrastructure for the following reasons:

a. The proposed definition refers to Management Systems used to initialize, deploy, **OR** configure but the definition of Management Systems states that, to be a Management System, it must initialize, deploy, AND configure. These two definitions presently conflict with each other. Before the

proposed definition of SCI can be accepted, the identified conflict between this term and its companion term (Management Systems) needs to be harmonized.

b. Currently the scope of SCI is unclear. An explanation of the limiting factors for the scope of SCI regarding their software should be provided. e.g., would the firmware of a server blade be included within the scope of SCI?

c. {C}We also suggest that the proposed definition would be more easily understood if language and terms were drawn from current NERC CIP acronyms rather than using their long form names.

d. {C}The term may not be clear or fully understood by all entities and we suggest adding examples within the Technical Rationale.

Interactive Remote Access: While EEI understands the need to streamline the definition of IRA, additional clarification is needed to better describe IRA in the context of virtualization, particularly regarding serial links. While some clarity has been provided within the Technical Rationale regarding serial to IP converter, it is silent on serial links that are used exclusively for polling purposes and have no interactive capability beyond providing requested data.

Management Systems: This definition appears to align with the definition of a hypervisor; however, it also includes some language that tries to straddle between both virtualized and non-virtualized environment. This ambiguity may create confusion, and EEI recommends the definition be clarified. It may also be helpful to include some examples of Management Systems within the Technical Rationale.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	No
Document Name	

Comment

We have a concern about the definition of SCI. In two places we say "one or more". The problem is what if both statements are answered with one and no more than one. It isn't clear when we say "One programmable electronic device (excluding Management Modules) and its software that share its CPU, memory, or storage resources with one BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets;" What happens when the device itself is a BCS? Is it sharing resources with itself and thus SCI and thus any physical stand alone box is SCI? Consider clarifying that the share is with something besides itself.

The Management Systems definition as written would include a Cyber Asset that maintains the integrity of another Cyber Asset, through control of the processes for configuring those assets, which would expand the scope of the definition beyond virtualization. Please see suggestions from Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 3/19/2021.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	
Comment	

Request keeping the ESP and EAP definitions in the active portion of the glossary. Having a section for retired terms will not help with compliance. We prefer a clear delineation.

Request clarification on Management Module and Management Systems – should the entity internally define “management and monitoring capabilities?” SCI definition use AND while the Management Systems definition uses OR. Request consistency.

Request clarification of SCI’s definition. The proposed definition of SCI could include network devices. SCI interpretations say that network services are not SCI.

Likes 0	
Dislikes 0	
Response	

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	
Comment	

Please see JEA coments, an individual response to my comment is not required.

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	

Intermediate System: N&ST suggests, “An Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access to only authorized users. The Intermediate System must be located outside the BCS’s logical isolation.”

ERC: N&ST suggests, “The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset that is outside of its associated logical isolation via a bi-directional routable protocol connection.”

Rationale: Clearer and more consistent with the revised definition of IRA.

Management Systems: N&ST suggests, “Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of one or more of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.”

Rationale: N&ST believes that specifying a system must be capable of managing all three of “initializing, deploying and configuring” in order to qualify as a “Management System” will set the stage for endless arguments about whether a given system does or doesn’t fit the definition. N&ST agrees with the SDT’s opinion that devices used to initialize, deploy, or configure EACMS performing logical isolation should be subject to CIP-005 R1 Part 1.2. However, the proposed definition creates a potential loophole which, we believe, should be eliminated.

Shared Cyber Infrastructure (SCI): N&ST believes the inclusionary language at the end of the proposed definition (“...including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.”) makes the definition confusing and possibly recursive (a Management System used to configure SCI is SCI?). We recommend removing “Management Systems” from the proposed definition. If the SDT believes Management Systems used to configure SCI should be subject to the same set of requirements as SCI, the SDT should consider adding them to the appropriate “Applicability” lists in each Standard.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

Please see our answer to #3.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Cyber Asset should not exclude Shared Cyber Infrastructure. It is just another type of Cyber Asset. Shared Cyber Infrastructure is really a Cyber Asset with a specific purpose.

Cyber Security Incident is written to introduce significant scope creep.

Interactive Remote Access should be reviewed to determine if the language, “User-initiated access by a person employing a remote access client” is still appropriate. There are many implementations that would meet the intent of Interactive Remote Access but may not use a traditional remote access client. If “remote access client” is still necessary, more definition should be provided for the wording.

Intermediate System should retain the wording of access control to restrict Interactive Remote Access to only authorized users. The revision could be unintentionally seen as restricting access from all users. There is no provision in the definition to allow access to anyone.

Virtual Cyber Asset should be clarified to note whether they are required to be on-premises or cloud. If it intended to allow for cloud, it would be beneficial to state that clearly. As written, it could be interpreted that a virtual appliances would be out of scope.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Conceptually, the ISO/RTO Council (IRC) Standards Review Committee (SRC) [1] supports the SDT and its efforts to expeditiously modify the CIP standards to accommodate the use of Virtualization and to more readily be able to adopt other future technological innovations. We believe this will pave the way for increased flexibility, upgradeability and security. In support of the SDT’s efforts, the SRC offers the following comments to assist the SDT in moving forward with this very important initiative.

Recommendation: To ensure entities can continue all or a portion of their existing programs without having to implement virtualization or undertake significant administrative changes, the SRC recommends the terms, Electronic Security Perimeter (ESP) and Electronic Access Point (EAP), be retained as an option for the following reasons:

1) **Ease of backward compatibility**. The concepts of ESP and EAP are well understood and consistently implemented by entities with well-known costs, documentation and audit requirements. Retention of the ESP and EAP concepts will provide a clear path for entities who choose to maintain status quo to remain compliant.

Regardless of whether the terms ESP and EAP are kept, auditors will want/need to know where the logical isolation zone begins and ends.

2) **Continued clarity**. Replacing ESP and EAP with an undefined term, “logical isolation,” will require individual entities to define “logical isolation” with unknown impacts to their existing program and audit requirements. While the IRC SRC sees a benefit to having a more open and flexible definition from the standpoint of being able to more readily adopt new technology and practices that can enhance the security of critical infrastructure, the related cost and compliance risk associated with this change may have the adverse effect of increasing resistance to change in order to avoid audit risk.

The IRC SRC sees a path forward whereby the SDT can introduce the use of the term “logical isolation” in concert with retaining the prior concepts of ESP and EAP by either:

A) Defining the term “logical isolation” to include the terms ESP and EAP as acceptable means of meeting this definition or

B) Reinstating prior language references to ESP and EAP in each applicable requirement and definition in the **Glossary of Terms Used in NERC Reliability Standards** that has been modified to introduce “logical isolation” and offer the prior language as an alternative acceptable means of continuing to comply with the requirement and meet the definition, respectively.

- **Cyber Security Incident** – as noted above, SRC recommends the definition be revised to accommodate prior ESP concepts.
- **External Routable Connectivity (ERC)** – as noted above, SRC recommends the definition be revised to accommodate prior ESP concepts.
- **Interactive Remote Access (IRA)** – as noted above, SRC recommends the definition be revised to accommodate prior ESP concepts.

Clarify the **Management Interface**, **Management Module** and **Management Systems** definitions as they are overly vague.

- **Management Interface** – SRC proposes the SDT narrow this definition to include only those interfaces that can be used to configure Cyber Assets.
- **Management Module** – Describe the type of devices in this category; e.g. out-of-band management devices, I/O devices, etc
- **Management Systems** – per the **Definitions and Exemptions Technical Rationale**, this term is intended to address “the unique risk for virtual environments presented by the management ‘consoles’ for such environments.” It then goes on to say the “intent is to define that capability and then include this within the definition of SCI.”

Recommendation: Clarify where management console servers fall; i.e. under Management Module or Management Systems? Note: the Management Systems definition explicitly excludes Management Modules.

- **Physical Access Control Systems (PACS)** – SRC is concerned that the defintion for PACS could be interpreted to mean that SCI could be solely responsponsible for controlling, alerting or logging access to a Physical Security Perimeter (PSP), even though the word “or” is used to denote that: “Cyber Assets, Virtual Cyber Assets, ***or*** Shared Cyber Infrastructure that control, alert, or log access to the Physical Security Perimeter(s)…”

Recommendation: SRC recommends the following change to the definition to clarify intent:

*Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that **collectively** 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.”*

- **Reportable Cyber Security Incident** - the “Currently Approved Definition” provided in the CIP Definitions document for Project 2016-02 does *not* match the current definition in the **Glossary of Terms Used in NERC Reliability Standards**; i.e. “*A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity."*

Recommendation: Clarify why it is necessary to change the definition for **Reportable Cyber Security Incident** if the underlying definition for **Cyber Security Incident** is modified. If it is unnecessary, leave the existing definition for **Reportable Cyber Security Incident** as is.

- **Self-Contained Application** – the SRC requests the SDT clarify the nature of “immutable software binaries.” During which stage of the software lifecycle is the software binary expected to be immutable?
- **Shared Cyber Infrastructure** - the definition seems to address specific scenarios involving storage and/or host virtualization infrastructure; however, may be interpreted more broadly to include sets of systems supporting configuration management and monitoring/ remediation support systems. It is not clear whether it was the SDT’s intent to include the latter systems.

Recommendation: Clarify the characteristics of “Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.” Would configuration management systems; e.g. Ansible Tower, Tenable Security Center or Tripwire Enterprise Console be considered Management Systems?

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP (with the exception of our response to question 5).

Likes 0	

Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC	
Answer	No
Document Name	
Comment	
Capital Power appreciates the opportunity to participate in stakeholder consultation on this project. While Capital Power supports modifications to CIP Reliability Standards and associated definitions that more clearly accommodate virtualization, it is imperative that legacy solutions remain in the standards for those entities who intend to continue to use those solutions. **Shared Cyber Infrastructure (SCI)** – Capital Power does not support the currently proposed definition for Shared Cyber Infrastructure for the following reasons:	

- The proposed SCI definition refers to Management Systems used to initialize, deploy, **OR** configure but the definition of Management Systems states that to be a Management System it must initialize, deploy, **AND** configure. These two definitions presently conflict with each other. Before the proposed definition of SCI can be accepted, the identified conflict between this term and its companion term (Management Systems) needs to be harmonized.
- Currently, the scope of SCI is unclear. An explanation of the limiting factors for the scope of SCI regarding their software should be provided, e.g., would the firmware of a server blade be included within the scope of SCI?
- The term SCI may not be clear or fully understood by all entities and we suggest adding examples within the Technical Rationale.

Virtual Cyber Asset (VCA) – Capital Power agrees with other stakeholder comments encouraging the integration of the concept of a VCA into a revised definition for Cyber Assets. As there are no additional or specific requirements for a VCA, the integration of this concept into the Cyber Asset definition removes unnecessary complexity.

- Proposed modification to **Cyber Asset (CA):** Programmable electronic devices, including the hardware, software, and data in those devices. This includes platforms operating virtual machines, which are logical instances of an operating system or firmware hosted on a physical platform.

Interactive Remote Access (IRA): The new definition of IRA no longer limits the applicability to routable protocols only. This may result in some additional communication types to be included in scope like serial over dial-up and potentially could have significant scope impact on entities compliance programs. Capital Power recommends that the SDT provide guidance regarding if this was the intent or if the use of the terminology 'user-initiated' was intended to point towards routable protocols.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

NRG agrees with most of the newly defined and retired terms. However, NRG believes that removing the term, “Electronic Securiry Perimeter” adds a bit of ambiguity and leaves several areas open to interpretation. NRG believes that a new defined term should be added to replace, “Electronic Security Perimeter”. One possible option could be, “Logical Isolation Zone”.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

NRG agrees with most of the newly defined and retired terms. However, NRG believes that removing the term, “Electronic Securiry Perimeter” adds a bit of ambiguity and leaves several areas open to interpretation. NRG believes that a new defined term should be added to replace, “Electronic Security Perimeter”. One possible option could be, “Logical Isolation Zone”.

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

Standards are becoming much more difficult to navigate with this terminology, inclusions and exclusions. The prescriptive nature tends to leave certain high risk Cyber Assets out of scope (vulnerability scanners and Tripwire for example). We do agree that management systems were excluded and that they are high risk, so we support their inclusion.

SMUD was already protecting our SCI without all of this prescriptive language and we do not agree with the 20% of the entities that were polled and said that the standards were holding them back. If this is the direction that the standards are going, we should consider adopting and already developed standard such as PCI rather than reinventing the wheel.

Likes 0	
Dislikes 0	

Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial_Comment_Form_01222021_gsoc - FINAL DRAFT.docx
Comment	

GSOC provides the following comments regarding the added, revised, and retired defined terms:

1. The definition of BCSI has been revised to include SCI, but not Management Modules or Management Interfaces. It would seem that, at a minimum, information about Management Modules could provide critical information about associated SCI and BCS. GSOC suggests that Management Module should be included in the definition of BCSI. If not, can the SDT provide its explanation for not including Management Module in the definition of BCSI?

2. Relative to Cyber Security Incident and Reportable Cyber Security Incident, both are revised to add the Shared Cyber Infrastructure (SCI), which excludes Management Modules and Management Interfaces, but not Management Systems. Would the attempt to compromise or compromise of an active Management Module in an attempt to access or disrupt the functions of SCI or BCS not merit reporting? This seems like a potential gap where these could be used to compromise related SCI or other cyber assets. GSOC suggests that Management Module should be included. If not, can the SDT provide their explanation or justification?

3. Electronic Access Control or Monitoring Systems should be revised to Electronic Access Control or Monitoring System to comport with its use in its singular form in other defined terms.

4. GSOC provides the following comments on the proposed revision of Interactive Remote Access:

a. The revision of Interactive Remote Access removes the ability to utilize technology other than remote access clients, which seems to militate against the level of flexibility available to facilitate the use of new and advanced technology.

b. The revision of IRA seems to obfuscate whether an “asset” is physical or logical in nature and whether being inside of a trusted network would be considered IRA. Clarification of the SDT’s intent relative to the revision is recommended.

5. The added terms regarding management module, management system, and management interface require some additional clarification to ensure that the distinctions between the new terms are clear and unambiguous. GSOC provides comment relative to the following:

a. Burying management systems in the definition of SCI may create confusion where it is intended to be or should be clearly correlated to other defined terms and requirements. It is recommended that – where such terms are utilized – they should be directly correlated to reduce the potential for confusion.

b. Suggest the following revision to the term “Management Interface” - A physical or logical interface of a Cyber Asset or Shared Cyber Infrastructure with the capability to manage and monitor the hosted Cyber Assets and the Shared Cyber Infrastructure.

c. Suggest the following revision to the term “Management Module” - An autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities of the function and health of the hardware underlying the Cyber Asset or Shared Cyber Infrastructure. This is independent of the host system's CPU, firmware, and operating system and any management or monitoring thereof.

d. Suggest the following revision to the term “Management Systems” - Any combination of Cyber Assets or Virtual Cyber Assets that control the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

e. Why do Management Modules not require PSP protection?

6. Is the exclusion noted in the definition of a Protected Cyber Asset necessary given that the initial criteria seems to require logical connection and, therefore, would already exclude assets that are not logically connected? Perhaps reformatting of the exclusions would increase clarity.

7. The definition of Self-Contained Application is not easily comprehended or relatable by non-technical personnel. As the reliability standards are intended for use by personnel across the utility industry, including compliance, legal, and other non-technical personnel, revision is recommended to make this defined term more universally understood.

Likes 2	Oglethorpe Power Corporation, 5, Johnson Donna; Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

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

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

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

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
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	
William Steiner - Midwest Reliability Organization - 10	

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 Cantwell - Lower Colorado River Authority - 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	
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	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	

Answer	Yes
Document Name	
Comment	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

2. CIP-005 Requirement R1 part 1.1 was revised to permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	
Conceptually, the SRC agrees with what the SDT is proposing; however, we don't think the language is clear enough to implement in practice. Controlled communications are undefined and could require significant effort by entities to interpret and define what is intended and essential to meeting this requirement. What happens if access is over-provisioned because an entity anticipates services are needed and then aren't used? Due to the vagueness of the language, it seems like this could happen quite readily. **Recommendation:** Clarify the definition so there is a level of consistency across the ERO.	

In addition, wording such as “e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE)” is difficult to understand. **Recommendation:** Replace this language with something in layman’s terms; e.g. “communications for substation automation systems.”	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Historically CIP-005 has related to the protection of the BCS. This should be the focus going forward. The applicable systems needs to be clarified that it only applies to PACS and EACMS that share infrastructure with something inside the ESP.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	No
Document Name	
Comment	

This draft requires PACS and EACMS on SCI to have logical protections, but not for all PACS and EACMS. This allows for human error when applying the standards as people will have to remember which rules apply to which since the rules were not applied in a uniform fashion. Additionally, the elimination of ESP will require extensive modifications to procedure, evidence, RSAWs, etc. Without ESP, how is the logical electronic security perimeter expressed?

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

NERC glossary term needed. The term 'logical isolation' is used in a range of different contexts across many industries. Is it similar to 'deny by default'? Is an ESP a subset of 'logical isolation'?

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Conceptually, the proposed change to only permit needed and controlled communications to and from applicable systems either individually or as a group is clear, however, it is unclear what it means to logically isolate all other communications. A clear understanding of the term logical isolation is needed to address this concern.

Additionally, EEI asks for clarification for the following:

- EEI asks for clarifications of the term “group” as used in Requirement R1, part 1.1. Currently, the Requirements of CIP-005-6 allow multiple BES Cyber Systems to exist within the same Electronic Security Perimeter. However, our understanding of proposed CIP-005-8 is that, when two or more BES Cyber Systems are 1) located within a Control Center; 2) utilizing a shared ESP; and 3) compliant under the current version of CIP-005, they may not be compliant under the proposed Requirements of CIP-005-8. This understanding is based on the potential inability to demonstrate control of communication between the two BES Cyber Systems. While we recognize that the intent may have been for those systems to be considered as part of a group, this is not clearly defined or explained. Without such clarification, entities may find it difficult to continue to use legacy systems under the proposed new Requirements.

- Applicability: PACS and EACMS are included when “hosted on SCI”. It is unclear whether PACS or EACMS hosted on standalone hardware would also meet this requirement. We recommend the language be clarified in proposed CIP-005 Requirement R1 part 1.1. (EEI also recommends evaluation of this issue with respect to R1.3, R1.4 and R1.5)
- Measures: EEI understands that if a VLAN is an acceptable logical isolation technique, then the device enforcing the VLAN would also need to be addressed. EEI requests clarification where these devices are within the proposed standard. (E.g., a switch with a VLAN that has a BCS connected to it. Would that switch be a high impact BCS? Or possibly SCI?) Please clarify how this concern has been addressed within the propose language of R1.1.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb 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; - Douglas Webb

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 2.

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 SRC.

In addition, PJM requests additional clarification on the “time-sensitivity” aspect of R1.1. This clarification may help entities determine any applicable exceptions.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	

Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed such that the entity first identifies needed communications, thenapplies control of the permitted communications.

Suggested language for R1.1 -

Identify needed communications and control permitted communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Likes 0	
Dislikes 0	
Response	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-005, R1, Part 1.1. PG&E does have concerns and supports the input provided by EEI.

Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	

SPP offers the following comments and questions for the SDT consideration for Question 2:

How would an entity logically isolate from its systems if the term ESP is removed? Recommend SDT consideration that there is no difference, but would require additional documentation and explanation on how network isolation is done, unless we define the two IP addresses as the isolation.

Recommend the SDT consider a definition of what Logical Isolation is, or offer clearly communicated examples.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions caused this no vote for this standard.

Would like clarification on if physical isolation is considered a type of logical isolation and if not, if it should be added as an applicable security control.

Would like clarification why the SDT choose to use “needed”, instead of “necessary” as used in CIP-003 R2 Attachment 1,Section 3.

There has been considerable push by some regions to have phone systems identified as BES Cyber Sytems. In their push, they want the possible threat of someone using calling in and pretending to have the authority to issues operational directives, to be considered in the BCS determination process. While we do not agree with this position, boic communication would be applicable for the R1.1 controls. Suggest including language that clearly exempts voice communication.

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

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	

Comment
FMPA supports the response submitted by TVA.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	

Comment
There is a lack of clarity around the expectation related to use of the term needed. If the intent of the SDT is to continue requiring documentation of “needed” communications, this should be converted to an explicit requirement stating the expected documentation rather than an implied requirement. If the intent is to continue the V5 expectations, document the communications services that are permitted (e.g. TCP ports, UDP ports, IP proctocols) with reason access is needed. If the intent is broader to address items such as services in a hypervisor, VLANs, VXLANs, it is not clear what is expected and appropriate language should be developed by the SDT. Further, when considering logically isolated networks that span multiple PSPs connected via a telecommuncations company, configuration is often not in the control of the entity.

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

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

The term controlled communications is not defined and open to interpretation. Is a router capable of performing controlled communications? Auditors may have differing opinions.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

There is no need to change a pre-established definition such as ESP. New application creates extreme confusion for application of security for cyber assets. Compartmentalization should be based on security enclaving but high watermarking. A VLAN should be highwater marked to Cyber Asset level as BES function will be impacted if it is compromised.

It seems SDT has compartmentalized assets in order to limit compliance application. Selective application of controls will result in significant security risks.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI's comments.

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	No
Document Name	

Comment

The Applicability in CIP-005 R1 Part 1.1 may contain a hall of mirrors for EACMS requiring an EACMS with the inclusion of “3. EACMS hosted on SCI” under the High and Medium Applicable Systems entries. One possible solution is to modify the inclusion to be something like:

“3. EACMS, not performing logical isolation, hosted on SCI.”

This would then become the corollary to the R1 Part 1.2 “EACMS performing logical isolation” inclusion. This change could solve the hall of mirrors and serve the security objective of requiring logical isolation of EACMS like Active Directory, where you can without requiring an EACMS for an EACMS that provides logical isolation.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The term “controlled communications” is new and is not defined. This term could be interperted in many different ways and does not have an industry accepted usage..

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	

JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP is concerned that the proposed change in CIP-005 Requirement R1 Part 1.1 is not clear without a clear understanding of the term logical isolation. AEP supports EEI's comments and asks clarification on the Applicability where PACS and EACMS are included when "hosted on SCI". It is unclear whether PACS or EACMS hosted on standalone hardware would also meet this requirement. Would this only be applicable if the SCI is hosting BCS or PCA that are mixed with PACS and EACMS on the same hardware? AEP recommends the language be clarified in proposed CIP-005 Requirement R1 part 1.1. AEP also recommends addressing this issue in R1.3, R1.4 and R1.5.	
Likes 0	
Dislikes 0	
Response	

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS agrees with the proposed change to only permit needed and controlled communication to and from appliable system wither individually or as a group is clear. We would like a clearer definition and understanding of what the term "logical isolation" means.	
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	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
The wording of the requirement is not clear. It states that entities are to permit only the needed and controlled communications but then goes on to state “logically isolate all other communications”. If only the needed communicates are allowed, what communications are being isolated? Other communications to non-CIP devices or systems? And why would this statement be needed? This would still be captured within the phrase of permit only the needed and controlled communications. Is the intent to prevent all other communications other than what is needed or to create a VPN or to encrypt the communication path? Additionally, the applicable systems column is not clear. Does the addition of routable protocols to the High Impact systems mean that if a High Impact system only has serial protocols (while unlikely) this requirement would not apply? This also creates another tier of systems: High with routable, High without routable, Medium with routable, Medium without routable, low, etc. Continuing to create tiers within the requirements complicates the requirements from an administrative standpoint without major security gains. Also, does the phrasing “hosted on SCI” for both PACS and EACMS mean that if a PACS or EACMS is not hosted on SCI that this requirement does not apply? Is this requirement only intended to apply to	

virtualized environments? The technical rational speaks heavily to logical isolation, but the requirement language and the language used in the applicable system column don't seem to completely line up.	
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 of adding virtual PACS and EACMS to the applicable systems since it expands the scope of the requirement. There is no documented reason for the scope increase. SIGE assumes that this change may be due to the possibility that BCS, PACS, and EACMS may use the same SCI. If that is correct, then SIGE proposes more specific language such as "PACS hosted on SCI that also hosts BCS; and EACMS hosted on SCI that also hosts BCS".	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE 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 changes of adding virtual PACS and EACMS to the applicable systems since it expands the scope of the requirement. There is no documented reason for the scope increase. CEHE assumes that this change may be due to the possibility that BCS, PACS, and EACMS may use the same SCI. If that is correct, then CEHE proposes more specific language such as “PACS hosted on SCI that also hosts BCS; and EACMS hosted on SCI that also hosts BCS”.

Likes 0	
Dislikes 0	

Response

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Proposed changes to R1 Part 1.1 are not required because the ESP concept can still be used with virtualization as one of the options.

Does a zero trust model make it difficult to do virtualization in other ways?

Would segmentation technology count as the control or as the firewall?

An ESP for each microsegmentation would be daunting to any entity.

Logical isolation is not a defined term. We would like to see an actual definition for "logical isolation"

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx

Comment

See attachment for comments.

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
The prior definition defined traffic as ERC, then had a requirement to pass that through an EACMS. The new definition adds 'through an EACMS' as a qualifier of the traffic, but falls short of requiring the traffic to pass through an EACMS. (Traffic not going through an EACMS would then not meet the definition of ERC, so the applicable requirements would then not apply.) Consider replacing 'through an EACMS' with 'across logical network isolation'.	
Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The appears to be some ambiguity of the additional compliance requirements which are correlate to the new terms which need to be more defined.	
Likes 0	
Dislikes 0	
Response	

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	
Comment	

We support the NPCC TFIST and RSC comments and submit the following additional comments:

What are intelligent electronic devices ? Please use define terms.

The requirement doesn't clearly state the creation (establish) of the logical isolation. The requirement should estasblish the logical isolation. In this context logical isolation is not define nor specified.

Suggest removing any reference to "communications using protocol IEC TR-61850-90-5 R-GOOSE" and simply state " excluding time-sensitive protection or control functions".

Likes 0	
Dislikes 0	
Response	

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

CHPD approves of the direction of performing logical isolation at either the individual or group level instead of requiring an ESP.

However, including PACS and EACMS hosted on SCI in the Applicable Systems creates differing requirements for virtualized PACS and EACMS and physical devices. It is also not backwards compatible with entities who have already virtualized PACS or EACMS and are compliant today but would not be under the draft requirements. Given that the SDT acknowledged during its recent webinar that the only reason it has not extended this requirement to all EACMS and PACS is that it would be outside the SAR, it is clear that this is not a virtualization-based change and is outside the SAR. Additionally, it creates an issue where the device performing the logical isolation of the EACMS or PACS is not a CIP device, and is not required to comply with the CIP standards, creating a hall of mirrors situation, such as a virtual firewall providing logical isolation for a domain controller (but not for any BCS).

Likes 0	
Dislikes 0	
Response	

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

Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed such that the entity first identifies needed communications, thenapplies control of the permitted communications.

Suggested language for R1.1 -

Identify needed communications and control permitted communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

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

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

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	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
The relationship between logical isolation versus the physical security perimeter or its extension through secure conduits is unclear. The notion of zone isolation and conduits (IEC62443) is absent or too abstract. Conduits or secure tunnels between two endpoints (which are secured by a physical perimeter) is not clear.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed such that the entity first identifies needed communications, then applies control of the permitted communications.

Suggested language for R1.1 -

Identify needed communications and control permitted communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

RF does not agree with the proposed changes for the following reasons:

a. With each system becoming its own ESP (zero trust) – mixing of CIP and non-CIP network traffic on local network segments is permitted.

b. Logical isolation is not defined, leading to diverse definitions between entities and regions, therefore, a definition of logical isolation is required. In addition, a significant concern is that an entity could implement logical isolation using only a host-based firewall and essential systems could be directly connected to the internet – a side effect breaking the definition of External Routable Connectivity and enabling entities to bypass many now-required protections.

c. The use and definition of “controlled communications” within P1.1 is not defined. The SDT inferred access control, however, this should be explicitly stated in the Requirement.

d. Remediation VLANs are not defined and may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.

e. Dormant VMs that could be either explicitly or inadvertently activated could lead to noncompliance if they are not properly identified.

f. Parent Images and Parent/Child Images are not defined terms and could lead to compliance issues regarding network access and/or identification of Cyber Systems.

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 of only permitting, either individually or as a group, needed and controlled communications to and from Applicable Systems. However, the full intent and scope of "logically isolate all other communications" is unclear absent a defined term for "Logical Isolation". This issue may be resolved by defining Logical Isolation and providing a clearer understanding of what is required here.

Additionally, Southern requests clarification for the following:

1. Applicability: PACS and EACMS are included when "hosted on SCI". However, those devices are also included in the definition of SCI; thefore, the requirement language equates to the following applicability:

a. This requirement applies to PACS and EACMS hosted on programmable electronic devices that share their software, CPU, storage, or memory resources between those hosted PACS or EACMS *AND* one or more (1) H/M BCS ***OR*** their associated (2) EACMS, (3) PACS, or (4) PCA.

b. Southern requests the SDT consider the concepts outlined in the following clarifying changes to the Applicable Systems column, which helps clarify the vastly broadening scope of these requirements to EACMS and PACS assets not previously required. This is potentially a major change, but is supported by our other comments in this posting addressing the lower risk profile posed by PACS assets and EACMS assets that only perform a monitoring function. The intent here is to more properly scope risk where stand-alone virtual PACS and EACMS on SCI are of a significantly lower risk than SCI hosting BCS (and virtual PACS on the same SCI). From a risk-based perspective, please consider these associations for Applicable Systems:

i. High and medium impact BCS connected to a network via a routable protocol and their associated:

1. PCA;

2. PACS hosted on the same SCI as the BCS; and

3. EACMS hosted on the same SCI as the BCS.

c. Southern requests the SDT consider the potential "Hall of Mirrors" that is achieved when the object of the requirement (an EACMS) that is used to "permit" and "logically isolate" communications is also subject to having the requirement enforced on itself as an Applicable System. For example – with an EACMS being the object of the requirement, how then does an entity also concurrently use a Cyber Asset(s) (i.e., a 2nd EACMS) to "permit" and "logically isolate" communications to the 1st EACMS?

i. This is exponentially more complicated in a virtualized environment and could force entities, who would not be able to achieve the requirement, to forgo the benefits of virtualization as this would result in endless amounts of dedicated virtual clusters on dedicated hardware for each Applicable System type.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
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 generally agrees with the proposed changes. The logical isolation requirements provide flexibility and a pathway to adopt technology and practices that can enhance security of critical infrastructure. However, ISO-NE recommends several changes to improve comprehension, readability, and compliance with the requirements. The SDT should define the term “controlled communications” for a consistent interpretation across the industry and Electric Reliability Organization (ERO). Undefined terms create varying definitions and interpretations that can lead to disputes and disagreements between a Registered Entity and the Regional Entities that represent the ERO. ISO-NE also recommends removal or replacement of the word “ensure” as this language and expectation is inconsistent with all other requirements.	
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	

Answer	No
Document Name	
Comment	
The phrase "Logically isolate all other communications" should be further explained or clarified. As written, this could lead to incorrect assumptions or interpretations. Logical isolation should be defined as well.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends a change control board process that any new communication to and from applicable BCS needs approval by a responsible individual (not the CIP Senior Manager) to ensure a proper change control process has been applied to key equipment that allows remote access from outside the BCS controlled perimeter or zero-trust model.	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	
In theory the concept is good, however, more clarification on the relationship between logical isolated zones and physical isolated zones will be required.	
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

Comments: The proposed changes to R1 part 1.1 are not required because the existing ESP language and concepts can still be used with virtualization.

1. The language “Permit only needed and controlled communications to and from applicable systems” is problematic because it exceeds what the SAR requires. This language is more based in security defense in depth (multi-layered security controls) but for CIP, routable protocol traffic control between CIP Cyber Assets within the ESP is not required.

2. If the SDT intended to allow a non-ESP model (e.g., zero trust model) for controlling routable protocol electronic communications ingress or egress a BCS, adding EACMS as an alternative option for CIP-005-6 R1.1 could resolve this issue. For instance, in the VMware zero trust model, VMware NSX using a transparent in-kernel stateful firewall to block traffic between VMs, the NSX platform could be identified as an EACMS resulting from our proposed EACMS revisions.

The rationale for discussing logical isolation is as follows:

- The logical isolation is not a defined term and very subjective and can be interpreted differently;

- For routable connectivity, ESP and EAP as one of the options still would apply to a VCA and can be used seamlessly based on existing language and concepts. The term logical isolation is not needed

- For the non-routable connectivity, the objective of the SAR was to address IRA related serial connection issues, which can be resolved by our proposed IRA revision (See our comment for QUESTION 1). Except for IRA related non-routable connectivity, the logical isolation between CIP Cyber Assets using layer 1 and layer 2 connectivity is not required by the SAR.

RECOMMENDATION: We suggest keeping the applicable systems and making the following change to the CIP-005-6 R1 part 1.1

- All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP, or

- All applicable Cyber Assets connected to a network via a routable protocol shall through an EACMS that denies all communications to and from other Cyber Assets by default if ESP model is not used.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	

Comment
The proposed revision to CIP-005 R1.1 is clear with the exception of “controlled communications.” If an entity permits needed communications via an ACL, does that mean it is controlled? The requirement text starts with “Permit only needed…” which appears to make “controlled” unnecessary. Additionally, logical isolation is not defined and is subject to interpretation.

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: The proposed changes to R1 part 1.1 are not required because the existing ESP language and concepts can still be used with virtualization. A. The language “Permit only needed and controlled communications to and from applicable systems” is problematic because it exceeds what the SAR requires. This language is more based in security defense in depth (multi-layered security controls) but for CIP, routable protocol traffic control between CIP Cyber Assets within the ESP is not required. B. If the SDT intended to allow a non-ESP model (e.g., zero trust model) for controlling routable protocol electronic communications ingress or egress a BCS, adding EACMS as an alternative option for CIP-005-6 R1.1 could resolve this issue. For instance, in the VMware zero trust model, VMware NSX using a transparent in-kernel stateful firewall to block traffic between VMs, the NSX platform could be identified as an EACMS resulting from our proposed EACMS revisions. The rationale for discussing logical isolation is as follows: • The logical isolation is not a defined term and very subjective and can be interpreted differently; • For routable connectivity, ESP and EAP as one of the options still would apply to a VCA and can be used seamlessly based on existing language and concepts. The term logical isolation is not needed • For the non-routable connectivity, the objective of the SAR was to address IRA related serial connection issues, which can be resolved by our proposed IRA revision (See our comment for QUESTION 1). Except for IRA related non-routable connectivity, the logical isolation between CIP Cyber Assets using layer 1 and layer 2 connectivity is not required by the SAR. **RECOMMENDATION:** We suggest keeping the applicable systems and making the following change to the CIP-005-6 R1 part 1.1 • All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP, or • All applicable Cyber Assets connected to a network via a routable protocol shall through an EACMS that denies all communications to and from other Cyber Assets by default if ESP model is not used.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP has a concern as the requirement is written for Vitural environment, and we do not see in the requirement where it written for the backward compatibility and no reference to the current standard.	
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 alternative wording to clarify the treatment of time-sensitive protections and control functions: *Permit communications that are needed to and from applicable systems either individually or as a group and isolate them from other communication channels. Exclude devices that communicate using control functions (power system automation) or time-sensitive network (TSN) protections (e.g, IEC 61850, GOOSE, SV, PTP)*	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not generally agree with the proposed modifications. The verbiage within this requirement appears to be too vague for consistent implementation. The Requirements must be made clear that current ESP models are compliant. Duke Energy suggests including examples in the Measures column that are consistent with current ESP definitions to reinforce that current approaches remain valid. The proposed language leaves possibility for auditors to disagree with entity application of controls and enforce controlled communications within existing “groups” defined by current ESP boundaries. Duke Energy suggests clarifying as follows “Identify and document logical isolation for applicable	

systems individually or in groups, and only permit needed and controlled communications across the identified isolation, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE)."

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

What are intelligent electronic devices? Please use define terms.

The requirement doesn't clearly state the creation (establish) of the logical isolation. The requirement should establish logical isolation. In this context, logical isolation is not defined nor specified.

Suggest removing any reference to "communications using protocol IEC TR-61850-90-5 R-GOOSE" and simply stay to excluding time-sensitive protection or control functions.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

AEPCO is signing on to ACES comments.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	Yes
Document Name	

Comment

LCRA is concerned with the conecept of backwards compatibility and Regional Entities interpretation of what acceptable evidence is.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments regarding CIP-005, requirement R1:

1. In the proposed revisions for CIP-005, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….."

2. Revise requirement R1.1. for clarity as follows:

Permit only controlled communications that are [necessary/needed] to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
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	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
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	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 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	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is concerned with removing the terms Electronic Access Point (EAP) and Electronic Security Perimeter (ESP) from the NERC Glossary of Terms without adequately addressing those concepts in the proposed “logical isolation” definition. The EAP and ESP concepts are known throughout industry and have been further clarified through repeated compliance engagements. As noted in its response to SDT Question No. 1 above, Texas RE believes that registered entities can implement virtualized environments within the existing EAP and EACMS framework today.

The SDT is proposing to remove these terms and replace it with the term “logical isolation,” which does not have a proposed definition. Texas RE recommends the SDT define the term “logical isolation.” In doing so, Texas RE further suggests the SDT clarify that the EAP and ESP concepts apply as part of the overarching “logical isolation” concept.

Finally, Texas RE recommends retaining the measure language, which states: “*a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP*.”

Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	

Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

3. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? 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

Consider revising Parts 1.2.1 and 1.2.2 to clarify controls for "Management Systems" and "Management Interfaces." The proposed language in Part 1.2.2 could be inappropriately interpreted to imply the management plane must have its own hypervisor.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The inclusion of virtualization concepts with newly defined Applicable Systems makes the requirements harder to understand and identify what is truly applicable. SRP doesn't like how all the standards increased in size due to these additions. SRP prefers to implement a way to account for virtualization without sweeping changes – similar to Low Impact. The attention given to virtualization feels over weighted compared to non-virtualized systems. This increases the burden on entities without virtualization to comb through the standards to find what is applicable.

The requirement is written for Vitural environment, and SRP doesn't see in the requirement where it written for the backward compatibility and no reference to the current standard.

SRP would like clarification on how the applicable systems, in particular EACMS, are expanded because of the SCI term.

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: We believe there are more efficient methods to meet the SAR. Refer to the comments in QUESTION 1 regarding existing definitions.

The term “Management Interface” already exists in the inherent properties of a Cyber Asset in the manner in which a Cyber Asset connects to the network – i.e., copper, fiber, wireless, etc.… If the intent was to address access to a Cyber Asset, the existing language covers these controls in electronic access – ports and services and authentication (EACMS).

The management system could fall within one of the existing CIP cyber asset classifications. Based on our proposed language to the R1 part 1.1, the SDT only needs to add EACMS to R1 part 1.2 to resolve the zero trust model scenario.

Recommendation:

- Restore current CIP-005-6 R1.2 Requirements language and add “or EACMS”. The Requirements language could be such as:

“All External Routable Connectivity must be through an identified Electronic Access Point (EAP) or EACMS controlling communications to and from the BES Cyber System.”

Comment: If SCI is hosting a similar trust BCS then the SCI would be high watermarked to that trust level and should be exempt from R1.2. If the concern is transient execution then it would not make sense that the VCA within the BCS would be sharing the same resources as well.

Recommendation: If this is not a security concern, then in a similar trust environment, Management Systems should be excluded from R1.2

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

The proposed revision to CIP-005 R1.2 does not provide clarity related to “controlled communications.” If an entity permits needed communications, does that mean it is controlled? The requirement text starts with “Permit only needed…” which appears to make “controlled” unnecessary. Additionally, the term logical isolation is not defined and is subject to interpretation.

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

Comments: We believe there are more efficient methods to meet the SAR. Refer to the comments in QUESTION 1 regarding existing definitions.

The term “Management Interface” already exists in the inherent properties of a Cyber Asset in the manner in which a Cyber Asset connects to the network – i.e., copper, fiber, wireless, etc.… If the intent was to address access to a Cyber Asset, the existing language covers these controls in electronic access – ports and services and authentication (EACMS).

The management system could fall within one of the existing CIP cyber asset classifications. Based on our proposed language to the R1 part 1.1, the SDT only needs to add EACMS to R1 part 1.2 to resolve the zero trust model scenario.

Recommendation:

- Restore current CIP-005-6 R1.2 Requirements language and add “or EACMS”. The Requirements language could be such as:

“All External Routable Connectivity must be through an identified Electronic Access Point (EAP) or EACMS controlling communications to and from the BES Cyber System.”

Likes 0	
Dislikes 0	

Response

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

Comment

Reclamation recommends the virtualization requirements contain direct and detailed references to associated physical security requirements that protect and manage the equipment containing the virtual systems. Without this information, field employees could erroneously focus only on the logical protections.

Reclamation also recommends physical security requirements be connected to their associated virtualization requirements with direct and detailed references to clarify what is being protected.

Technical Guidance talks about the new term Management Interface being protected as described in CIP-005 R1 P1.2, but the redline for CIP-005 R1 P1.2 has no mention of the term Management Interface (only refers to Management Module). The Technical Guidance describes that Management Module will be addressed in CIP-005 R1.5, but there is not mention of Management Module in this Requirement.

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 generally agrees with the proposed changes. However, the requirement for anti-affinity rules for Management Systems appear to be overly burdensome and may outweigh any security benefit. We recommend allowing Management Systems to share memory and CPU with high-watermarked BES Cyber Systems as it still provides adequate security and eliminates the need for a physical host that would serve a single VM in many cases. Additionally, as with the other proposed modifications, the “Applicable Systems” column should be reviewed for clarity, consistency and readability.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
RF does not agree with the proposed changes for the following reasons: As with other Standards and Requirements, a definition of logical isolation is required.	

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed such that the entity first identifies needed communications, then applies control of the permitted communications.

Suggested language for R1.2.2 -

1.2.2. Identify needed communications and control permitted communications to and from Management Interfaces and Management Systems, logically isolating all other communications.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
Although we agree with the proposed requirement, we are concerned with the lack of clarity in the examples provided in the Measures for R1.2. Specifically, we would encourage the SDT to consider replacing the first bullet with “Logically isolated out-of-band network infrastructure configuration (firewall, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, other Layer 2/Layer 3 controls, multi-tenant environment, or encryption).	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Request clarification of requirements (1.2.1, 1.2.2, 1.2.3) with applicable systems such as EACMS. Do these requirements (1.2.2, 1.2.3) apply to the “management interface” without “management systems”?	
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	
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	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
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	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed suchthat the entity first identifies needed communications, then applies control of the permitted communications. Suggested language for R1.2.2 - 1.2.2. Identify needed communications and control permitted communications to and from Management Interfaces and Management Systems, logically isolating all other communications.	
Likes 0	

Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Best practices for vSphere suggest virtualizing vCenter (a Management System). However, for smaller entities who may only have a handful of Management Systems, requiring these systems to not share CPU and memory with other systems eliminates many of the benefits of virtualization and increases the complexity for no real tangible gain. This is compounded if the entity wants to implement best practices and have redundant Management Systems. Additionally, there are additional protections that are not accounted for by the proposed requirement, such as isolating the SCI from the internet or other controls that would mitigate such issues. See comments for question 19.

The language here creates a confusing scoping issue. The entity must look to three places to determine if a device must comply with the requirement, first the Applicable Systems column to find the “applicable system” (despite the fact the applicable system itself is not the device that needs to comply), the text of the requirement then to find which device actually needs to comply, and finally the definition Management System/Interface to see which devices meet that definition. Instead, the SDT should scope the Management System/Interfaces in the Applicable System column. That would allow the SDT to include logical isolation of Management Systems/Interfaces in CIP-005 R1.1 and isolation of BCS from Management System/Interfaces could be its own requirement part. For example, the Applicable Systems text could read, “Management Systems of SCI (and associated Management Modules) hosting High or Medium BCS or their associated: PCA; PACS; or EACMS”.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Applicable system mentions “management modules of SCI”. Requirements mention “Management system”, “Management Interface”. Those management reference three different definitions. Request clarification on the requirements (1.2.1,1.2.2,1.2.3) on management modules of SCI

With the new definition of EACMS (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the logical isolation of BES Cyber Systems), why specify “EACMS that perform logical isolation for a High Impact BCS“, its clear that and EACMS is a logical isolation.

Likes 0	
Dislikes 0	

Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The added complexity of Part 1.2, the retirement of the defined term 'EAP' has expanded the scope from devices strictly residing in an ESP to additional network segments which were previously not in-scope with the requirement The appears to be some ambiguity of the additional compliance requirements and the new terms.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	
Response	

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
There are more efficient ways methods to meet the SAR. Existing deifnitions should be revisited. The management system will fall within one of the existing CIP cyber asset classifications. As stated earlier, Basin would be in support of keeping the conceot of EAC and EACMS depending on how they define and write up EAC and EACMS.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
The proposed language in R1.2.2. and R1.2.3 seems to be contradictory given that R1.2.2 permits and R1.2.3 denies communications to and from Management Interfaces and Management Systems. CEHE suggests that the SDT consider clarifying the intention of the requirements.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
The proposed language in R1.2.2. and R1.2.3 seems to be contradictory given that R1.2.2 permits and R1.2.3 denies communications to and from Management Interfaces and Management Systems. SIGE suggests that the SDT consider clarifying the intention of the requirements.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS generally agrees with the proposed change to establish logical isolation requirements for Management Systems, Management Interfaces and associated SCI. We would like a clearer definition and understanding of what the term “logical isolation” means. Are the examples provided in the parenthesis, valid examples of logical isolation, ACL/VLAN/VXLAN/MPLS/VRF/multi-context, or multi-tenant environment.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP is concerned that the requirements containing the term logical isolation present a potential ambiguity for determining compliance. Logical isolation should be defined to ensure entities can achieve the performance-based requirement. AEP fully supports EEI’s suggestions, copied below for reference. Specific Comments:	

Requirement R1, Part R1.2

Please clarify how Requirement R1, Part R1.2 might apply to substation environments where no SCI exists.

1.2.1: The proposed definition of “Management System” lacks sufficient clarity (see our response to Question 1). We understand Management System to mean hypervisor. If this understanding is correct, the management system is what defines CPU/memory usage for its child VCAs. From this perspective, we request clarification on how management systems would restrict CPU/memory usage of other management systems and whether this is intended to be used for cloud-type services. To resolve this issue, the current language for this requirement should be clarified with additional explanation provided in the Technical Rationale.

1.2.2: AEP asks for clarification on why Management Modules have not been included in the language for this requirement, along with Management Interfaces and Management Systems. We note that Management Modules are included in the Applicability and Measures section but not in the Requirements. Please clarify whether this was intended and why or whether this was an oversight.

1.2.3: It appears that Part R1.2.2 already requires limiting the communication to Management Interfaces and Management Systems. Should this requirement be understood to mean that all communications to these Management Interfaces and Management Systems from BCS and their associated PCAs is to be denied? AEP requests clarification for this requirement.

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	No
Document Name	

Comment

As written, this standard appears to require that Management Interfaces be configured with logical isolation from the BCSs. It is unclear what security benefit this achieves. Management Interfaces in the same VLAN as BCSs would be as secure as the BCSs, therefore access to the Management Interface would be restricted even in that configuration. We would prefer to have the option of configuring Management Interfaces in the same VLAN as BCSs.

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	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Requirement R1.2 applies to EACMS that perform logical isolation for a High or Medium Impact BCS. EACMS could be a traditional firewall or a virtual firewall. R1.2.3 may cause confusion and prevent entities from communicating their EACMS (traditional firewall in this case) from within an ESP, such as BGP. Suggest clarifying that R1.2 is only applicable to virtual constructs, or R1.2.3 is only applicable to management access only.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No

Document Name	
Comment	
System should continue to follow security model of complete distrust. Only communication that is required must be allowed. This can only be established if rules are explicit including, Source, destination, Ports and Protocol. New application is very subjective and confusing. Industry is currently using Goose and still compliant, why change configuration and standards must be technology neutral.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We feel that a separate Part should be written in regards to SCI, leaving the existing CIP-005 Part 1.2 as currently written.	
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	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	

Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
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	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-005, R1, Part 1.2. PG&E does have concerns and supports the input provided by EEI.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed suchthat the entity first identifies needed communications, then applies control of the permitted communications.

Suggested language for R1.2.2 -

1.2.2. Identify needed communications and control permitted communications to and from Management Interfaces and Management Systems, logically isolating all other communications.

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 SRC.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb 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; - Douglas Webb

Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 3.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

General Comment: The requirements containing the term logical isolation represent a potential ambiguity for determining entity compliance. Logical isolation should be defined to ensure entities can achieve the performance-based requirement. (see our comments within Question 1).

Specific Comments:

Requirement R1, Part R1.2

Please clarify how Requirement R1, Part R1.2 might apply to substation environments where no SCI exists?

1.2.1: The proposed definition of “Management System” lacks sufficient clarity (see our response to Question 1). We understand Management System to mean hypervisor. If this understanding is correct, the management system is what defines CPU/memory usage for its child VCAs. From this perspective, we request clarification on how management systems would restrict CPU/memory usage of other management systems and whether this is intended to be used for cloud type services. To resolve this issue, the current language for this requirement should be clarified with additional explanation provided in the Technical Rationale.

1.2.2: EEI asks for clarification on why Management Modules have not been included in the language for this requirement, along with Management Interfaces and Management Systems. We note that Management Modules are included in the Applicability and Measures section but not in the Requirements. Please clarify whether this was intended and why or whether this was an oversight.

1.2.3: It appears that 1.2.2 already requires limiting the communication to Management Interfaces and Management Systems. Should this requirement be understood to mean that all communications to these Management Interfaces and Management Systems from BCS and their associated PCAs is to be denied? EEI requests clarification for this requirement.

Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	

Answer	No
Document Name	
Comment	
NERC glossary term needed. The term 'logical isolation' is used in a range of different contexts across many industries. Is it similar to 'deny by default'?	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	No
Document Name	
Comment	
PNMR agrees with comments from Joshua Andersen, On Behalf of: Salt River Project, WECC, Segments 1, 3, 5, 6	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	

Comment
Request a better separation for Requirements between SCI and locally managed for non-SCI. By including EACMS there will be additional work required to segment the networks between the IRA and management networks and would bring into scope more of the IT network. Additionally, we propose this as a different definition for IRA: Authenticated access (a person/human) to the BCS from a VCA outside the logical isolation zone containing the BCS.

Likes 0	
Dislikes 0	

Response

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

Comment
Please see comments in response to Question No. 2.

Likes 0	
Dislikes 0	

Response

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

Comment
Conceptually, the SRC agrees with what the SDT is proposing; however, CIP-005, R1, Part 1.2 envisions the segmentation of the management plane. What if the management plane cannot be separated? There should be allowance for this possibility. **Recommendation:** Modify Part 1.2 as follows: **1.2.1** “Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per ***Cyber Asset*** capability.” **1.2.3** “Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per ***Cyber Asset*** capability.”

Likes 0	
Dislikes 0	

Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the proposed modifications. However, the proposed applicability may be confusing. Is SCI hosting only EACMS subject to requirements beyond that which presently applies to physical EACMS? Duke Energy in concerned that the inclusion of physical EACMS in the applicability of this requirement represents a significant expansion of scope. It appears that management interfaces of substation firewalls would go from having no specific network-based CIP requirements to being relevant for additional restrictions that would present a high management burden. It is unclear whether local ACLs on those management interfaces would be sufficient to meet the new requirement. Additionally, the requirement for anti-affinity rules for Management Systems appear to be overly burdensome in relation to the purported security benefit – allowing them to share memory and CPU with high-watermarked BCS provides adequate security and eliminates the need for a physical host that would serve a single VM in many cases. System capability is inadequately defined in this context (for example, is a two-host cluster with one host in maintenance mode given a “capability” waiver for allowing a resident virtual management system to share the remaining active physical host with virtual BES Cyber Assets?).	
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 supports the SDT’s proposed direction in R1.2, and requests the SDT to consider the following with regard to the use of these two statements used throughout CIP-005:	

1. “Permit only needed and controlled communications to and from…”

2. “Logically isolate all other communications…”

Here, the act of “permitting only needed and controlled communications” is also a form of “logical isolation.” We suggest the SDT consider the below proposed modifications for multiple requirements that carry this former language:

1. “Implement Logical Isolation to permit only needed and controlled communications to and from XYZ … and deny all other communications.”

Southern also reiterates that the requirements for logical isolation represent a potential compliance risk for applicable entities because the term is undefined, making the reliability objective unclear for the industry to ensure their processes will pass regulatory inspection. We encourage the SDT to define Logical Isolation to ensure entities can achieve the performance-based requirement.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments regarding CIP-005, requirement R1.2:

1. In the proposed revisions for CIP-005, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., “…hosting [] impact BCS and the BCS’s associated …..” or “….hosting [] impact BCS and the SCI’s associated…..”

2. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

3. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

4. It is unclear why Management Modules are included in the applicable systems column of Requirement R1.2 when they are not specifically addressed in the requirements in the next column whereas other applicable systems are. Revision may be necessary to ensure clarity and consistent application and understanding.

5. Revise requirement 1.2.2. For clarity as follows:

Permit only controlled communications that are [necessary/needed] to and from Management Interfaces and Management Systems, logically isolating all other communications.

4. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

AEPCO is siging on to ACES comments.

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
The applicable system mentions “management modules of SCI”. Requirements mention “Management system”, “management Interface”. That management references three different definitions. Request clarification on the requirement (1.2.1, 1.2.2, and 1.2.3) on a management module of SCI. With the new definition of EACMS (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of logical isolation of BES Cyber Systems), why to specify “EACMS that perform logical isolation for a High Impact BCS”, it’s clear that and EACMS is logical isolation.

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

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

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	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
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	
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	

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	
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	
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	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 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	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
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	
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	
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, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE agrees that there should be CIP applicable Requirements and Parts for Management Systems, Management Interfaces, and associated SCI. Although not specifically related to virtualization, Texas RE recommends Management Modules should also apply to BCAs, PACS, and EACMS that are not on the SCI. Texas RE seeks clarification on whether management modules on current applicable BCAs, PACS, EACMS that are not on SCI are applicable to the CIP Requirements and Parts in the Applicable Systems column.

Likes 0	
Dislikes 0	

Response

4. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Please see comments in response to Question No. 2. As written, including PACS will be an issue because PACS are not required to be within a PSP and actually control the PSP.	
Likes 0	
Dislikes 0	
Response	

Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	

Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	No
Document Name	
Comment	
While it might fulfill the directive from FERC, it is unclear what technology would be used to accomplish this. Would we need to create IPSEC tunnels between switches on the same network but in different PSPs and have cabling traversing those PSPs? Or does the SDT believe something like IPv6 to be a valid way of complying with this requirements?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI is concerned that the change that moved CIP-006 R1.10 to CIP-005 R1.3 has created some unintended reliability gaps that appear to exceed the scope of the Project 2016-02 SAR. In CIP-006-6, Requirement R1, Part 1.10 specific changes were made to satisfy FERC Order 791, paragraph 150 regarding access physical restrictions to cabling and other nonprogrammable communications components used for connection between appliable Cyber Assets within the same ESP. Among the applicable systems identified to satisfy this Commission-mandated change included “Medium Impact BES Cyber Systems at Control Centers and their associated PCA”. However, the new requirement in CIP-005 R1.3 does not duplicate this requirement and fails to specifically include language identifying Medium Impact BES Cyber Systems at Control Centers. EEI recommends the restoration of the CIP-006 Requirement R1, Part 1.10 in its entirety or modify CIP-005 to fully address the identified reliability gap.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	No
Document Name	
Comment	

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 4.

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

Exclusions have an undefined term. Proposed Requirements address some of the protections of a communication network without defining it.

Request removing specific technologies like encryption.

Request new wording on the exclusion of CIP-012 and time-sensitive protocols since Real-time Assessment and Real-time Monitoring are not clearly defined.

The proposed change isn't in relation to the SAR. The requirement should have stayed in CIP-006, furthermore, the new requirement isn't in tune with the old requirement.

Suggest removing any reference to "communications using protocol IEC TR-61850-90-5 R-GOOSE", what about other similar protocols.

Suggest removing any reference to "CIP-012".

Suggests stating the exclusion to *time-sensitive protection or control functions*, which is the common language.

Suggest removing any reference to "physical controls" as the concept of implementing confidentiality and integrity controls can include physical controls.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We agree with the changes for CIP-005 R1 Part 1.3.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-005, R1, Part 1.3. PG&E does have concerns and supports the input provided by EEI.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions caused this no vote for this standard.

The “Physical controls that restrict access to the cabling and other nonprogrammable communication components,” should be moved to CIP-006 with all other physical security controls.

Request new wording on the exclusion of CIP-012 and time-sensitive protocols since Real-time Assessment and Real-time Monitoring are not clearly defined.

The exclusion for CIP-012 should be expanded to also exclude communication to a Control Center owned by others. The current language seems to require a GO with only a control room, to encrypt their communication to an LCC or ISO.

Suggest excluding voice communications as is done in CIP-012

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	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
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 modified requirement covers all medium and high impact BES Cyber Systems. The former requirement's scope was limited to high BCS and medium impact BCS at Control Centers. This would require significant changes to BES facilities with medium impact BCS which are not Control Centers, such as large generation facilities which have disperse PSPs. This change is not in the scope of the SAR and should be updated such that the scope is limited to the prior version.	
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	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Remove the reference to encryption. This could be added to measures for this requirements	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
Applicability section is confusing. Too much compartmentalization of devices and non-industry standard definition are not needed. BCS definitions should be updated to address logical assets and apply high watermarking. **Current approach limits security with assumption that associated devices can be compromised externally, but BES impact must be considered if Cyber system is compromised and made unavailable.**	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI's 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	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AEPCO is signing on to ACES comments, please see below: The modified requirement covers all medium and high impact BES Cyber Systems. The former requirement's scope was limited to high BCS and medium impact BCS at Control Centers. This would require significant changes to BES facilities with medium impact BCS which are not Control Centers, such as large generation facilities which have disperse PSPs. This change is not in the scope of the SAR and should be updated such that the scope is limited to the prior version.	
Likes 0	
Dislikes 0	

Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP fully supports EEI's comment with the concern that the change of moving CIP-006 R1.10 to CIP-005 R1.3 has created some unintended reliability gaps that appear to exceed the scope of the Project 2016-02 SAR. As noted in EEI's comments, specific changes were made in CIP-006-6, Requirement R1, Part 1.10 to satisfy FERC Order 791, paragraph 150 regarding access physical restrictions to cabling and other nonprogrammable communications components used for connection between applicable Cyber Assets within the same ESP. Among the applicable systems identified to satisfy this, Commission mandated change included "Medium Impact BES Cyber Systems at Control Centers and their associated PCA". However, the new requirement in CIP-005 R1.3 does not duplicate this requirement and fails to specifically include language identifying Medium Impact BES Cyber Systems at Control Centers.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS would like to know if the amendments to CIP-005 R1.3 porting over from CIP-006 R1.10 exceed the scope of the SAR, due to the lack of the language to medium impact at control centers?	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by Duke Energy and submits the following comment for consideration:	

MPC requests a clarification on the intent of the changes to CIP-005 R1.3. The proposed language would require physical protections for data traversing communication links between two adjacent PSPs within a substation control yard with no virtualization present. This effectively extends CIP-006-6 R1, part 1.10 to medium impact BES Cyber Systems. Is this the intent of the drafting team? The SAR does not contain any language that would support this change when virtualization is not present.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The proposed Requirement, R1 Part 1.3, states that the use of encryption or physical controls are acceptable; however, the Measures do not state that evidence may include proof of physical controls. The SDT needs to include evidence of physical controls in the Measures section, such as,

“Evidence may include, but is not limited to:

• architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption), or

• documents detailing the physical control methods used to restrict access to the cabling and other nonprogrammable communication components.”

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
The proposed Requirement, R1 Part 1.3, states that the use of encryption or physical controls are acceptable; however, the Measures do not state that evidence may include proof of physical controls. The SDT needs to include evidence of physical controls in the Measures section, such as, “Evidence may include, but is not limited to: • architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption), or • documents detailing the physical control methods used to restrict access to the cabling and other nonprogrammable communication components.”	
Likes 0	
Dislikes 0	
Response	

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
As stated earlier, Basin would be in support of keeping the conceot of EAC and EACMS depending on how they define and write up EAC and EACMS.	
Likes 0	
Dislikes 0	
Response	

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	

Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
“Physical controls” as used in the requirement is unclear. NIPSCO requests that the SDT provide clarity on what “physical controls” entail. Examples of such controls would be valuable. For example, is jacketed fiber a sufficient physical security control, and in what situation(s)?	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
We support the NPCC TFIST and RSC comments and submit the following additional comments: The proposed change isn’t in relation to the SAR. The requirement should have stayed in CIP-006, furthermore, the new requirement isn’t in tune with the old requirement. Suggest removing any reference to “communications using protocol IEC TR-61850-90-5 R-GOOSE”, in order to take into consideration other similar protocols?	

Suggest removing any reference to “CIP-012”

Suggest stating the exclusion to *time-sensitive protection or control functions*, which is common language.

Suggest removing any reference to “physical controls” as the concept of implementing confidentiality and integrity controls can include physical controls.

Likes 0	
Dislikes 0	

Response

Victoria Mordi - Entergy - 3,7,9 - SERC

Answer	No
Document Name	

Comment

REDLINE: ‘R1 Part 1.3...Protect the data traversing communication links, where the logical
isolation spans multiple Physical Security Perimeters, through the use of:
confidentiality and integrity controls (such as encryption)...”Is one interpretation that we will have to encrypt between Medium and High? If “yes” to this, then Entergy response is to clarify the requirement further... Entergy is currently not in a position to encrypt
from Medium to High... If “no”, then Entergy is in agreement with NERC proposal.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CHPD supports the move of CIP-006 R1.10 to CIP-005, as it was not really a physical security requirement. The language still fulfills the directive of Order 791.

However, as with CIP-005 R1.1, the inclusion of PACS and EACMS hosted on SCI is not consistent with the SAR and should be removed. Additionally, the scope has been expanded to beyond Control Centers, which should be removed.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with the changes for CIP-005 R1 Part 1.3. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
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	
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	
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

Having added “where logical isolation spans multiple physical security perimters” excludes a lot of traffic. Not sure why this is limited to traffic that is logically isolated vs all traffic which appears to be the intent of the ferc order. It would be good to narrow the traffic down to traffic that is crossing network equipment managed by a third party, a carrier, or communication links shared with other entities.

We do not feel that the standard addresses the protection of the non programmable aspect of communication networks as currently written because of the wording “where logically spans…”

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

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

The requirement should have stayed in CIP-006, furthermore, the new requirement isn’t in tune with the old requirement.

Likes 0	

Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
RF believes there should be a minimum level of encryption required to ensure that older, less secure methods of encryption are not used.	
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 modifications to CIP-006-6 R1.10 and moving it to CIP-005-8 R1.3 to continue to satisfy the Commission's directive in FERC Order 791 (paragraph 150.). Specifically, the deletion of CIP-006, Requirement R1, Subpart 1.10 and the development of a new requirement within CIP-005-8 (i.e., Requirement 1, Subpart 1.3) to protect "nonprogrammable" communication devices within networks that span multiple PSPs, per FERC Order 791, paragraph 150, *is achievable if simply relocating a requirement*. However, Southern questions the SDTs intent in removing medium impact BCS at Control Centers as an Applicable System, and replacing it with medium impact BCS connected to a network via a routable protocol. This alone has the potential to greatly increase the scope of the former CIP-006-6 R1.10 requirement, and the risk reduction or BES reliability benefit is not fully understood.	

Additionally, Southern fails to see the need to add PACS and EACMS hosted on SCI, and the SCI hosting those PACS and EACMS, to the Applicable Systems column. Southern requests the SDT provide additional context into these additions from the former CIP-006-6 R1.10 requirement; specifically, is there commensurate increase in risk and probability for EACMS and PACS warranting this scope expansion? Is there a reliability benefit to "protect the data" traversing communication links between two or more PACS or EACMS assets residing on the same SCI if that SCI physically spans more than one PSP, but that does not apply when these are physical stand-alone assets? To now add EACMS and PACS data protections is an unexpected scope expansion, and the risk reduction or BES reliability benefit is not clearly understood.

Under R1.3, the SDT appends the phrase "connected to a network via a routable protocol" for medium impact BCS, but does not also use this phrase for the high impact BCS, which it did use under R1.1. Is there a specific purpose for this omission here in R1.3?

Additionally, the SDT appears to be inconsistently using the conjunctions "and" and "or" within the Applicable Systems column. For example – R1.1 uses "**AND** their associated:", but R1.2 uses "**OR** their associated:" and R1.3 uses both "and" and "or" when describing associated Cyber Assets as Applicable Systems. Is this inconsistency intentional?

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

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 agrees that the revisions to the requirement address some of the reliability concerns raised as an issue in FERC Order 791, but ISO-NE does not believe that the revisions fulfill the directive from paragraph 150. The term "communication networks" needs to be defined, but there has been no attempt to do so in the revisions.

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	
Answer	No
Document Name	
Comment	
Consideration should be given to add "an equally effective logical protection" in the requirements which will allow for addtiional solutions to address the requirement.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends that Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and other BES Cyber Systems could be housed within virtual machines providing the same functionality residing locally on entity-owned computer hardware. Demarcation points of physically separated hardware and communication pathways between virtualized environments must be robust, redundant, and physically separated. Reclamation recommends virtual firewall appliances be used to segregate High/Medium/Low Impact systems in virtual environments. If virtual firewalls are used, mixed trust environments may not be an issue but hardware and supporting systems will need to be protected physically and electronically at the highest system impact level residing on the physical hardware. Reclamation also recommends that with Standards working on a zero-trust model there needs to be a documented approval process above technical support staff to make changes and approve any trust relationships.	
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	

Comments: The proposed language to addresses CIP-006-6 R1.10, exceeds the SAR. There is a current exclusion for communications equipment and links between ESPs – which implies multiple physical locations. If the SDT intended to address the exclusions of discrete communications links between ESPs, then we suggest a revision to CIP-006-6 R1.10. If NERC is interested in addressing confidentiality and integrity between multiple ESPs (i.e., a super ESP), then we suggest a new SAR to add additional requirements.

Recommendation:

- Restore current CIP-005-6 R1.3 language to retain the EAP and revise to include EACMS. Requirement language could be “Utilize an EAP or EACMS, to require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.”

Suggest changing the Applicable Systems for CIP-005-6 R1.3 to:

“High Impact BES Cyber Systems and their associated:

- PCA

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

• PCA”

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: The proposed language to addresses CIP-006-6 R1.10, exceeds the SAR. There is a current exclusion for communications equipment and links between ESPs – which implies multiple physical locations. If the SDT intended to address the exclusions of discrete communications links between ESPs, then we suggest a revision to CIP-006-6 R1.10. If NERC is interested in addressing confidentiality and integrity between multiple ESPs (i.e., a super ESP), then we suggest a new SAR to add additional requirements.

Recommendation:

- Restore current CIP-005-6 R1.3 language to retain the EAP and revise to include EACMS. Requirement language could be “Utilize an EAP or EACMS, to require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.”

Suggest changing the Applicable Systems for CIP-005-6 R1.3 to:

“High Impact BES Cyber Systems and their associated:

- PCA

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

• PCA”	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

1. SRP in general, the inclusion of virtualization concepts with newly defined Applicable Systems makes the requirements harder to understand and identify what is truly applicable. SRP doesn’t like how all standards increased in size due to these additions. SRP would prefer to implement a way to account for virtualization without sweeping changes – similar to Low Impact. The attention given to virtualization feels over weighted compared to non-virtualized systems. This increases the burden on entities without virtualization to comb through the standards to find what is applicable.

2. SRP reads the rational to imply that the communications need to be encrypted if the communications link is provided by a 3rd party, however the verbiage of the standard excludes that detail. Is encryption required if the communications infrastructure is soley under the control of SRP?

3. Does SRP need to encrypt the communications to the multiple PSPs, or can we protect the links with a harden conduit between both PSPs – more of an explanation is needed. It mentions protect the data traversing communication links, where the logical isolation spans multiple PSPs.

4. SRP request the clarification on third party communications, and devices not within the PSP. Standard does not specifically call out third party communications. Standard is not specific in listing what equipment or types of equipment and what communication links are included.

5. SRP considers this requirement to be written for both Physical and Virtual environemnts.

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

Entities should have the flexibility to utilize emerging technologies to protect data in transit.

Likes 0	
Dislikes 0	

Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not generally agree with the proposed modifications. It is not clear how this impacts existing compliance postures for CIP-006 R1 for ESPs that span multiple PSPs. It appears there may be a significant scope expansion based on the new applicability as written to Medium BCS at Generation facilities, with limited reduction of risk. Duke Energy believes the proposed language to address CIP-006 R1.10 potentially exceeds the scope of this SAR.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	Yes
Document Name	
Comment	
Proposed CIP-005, Requirement R1, Part 1.3 partially addresses the reliability gap raised in FERC Order 791, paragraph 150; however, it does not define “communication networks,” so that aspect remains outstanding. **Recommendation:** To address FERC’s concern, define the term “communication networks."	
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 SRC.

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

Issue 1:

The intent of removing CIP-006 R1 Part 1.10 in favor of a single requirement to address this security objective of ensuring the confidentiality and integrity of data when moving across unprotected physical space is positive, however the Applicability of the Requirement parts differs. CIP-006 R1 Part 1.10 applies to Control Centers only, and this change will force additional locations to be secured that are not currently required.

Issue 2:

Tacoma Power requests the SDT provide clarification on their intent for using the language “confidentiality and integrity controls (such as encryption)” rather than the general language of “encryption”. It would be helpful if the SDT would provide guidance on what type of evidence can be used to meet the confidentiality and the integrity in the Measures column for this Requirement. For example, an entity may choose to use an IPSEC Site-to-Site VPN to secure communications. The IPSEC VPNs are configured to use IKE v2 with AES256 encryption to provide confidentiality and certificates for authentication to provide integrity for the link. Is this the type of evidence the SDT is looking for to meet the requirement, or is simply providing evidence the link is encrypted sufficient to meet the SDT’s intent for using the confidentiality and integrity controls language? Suggest including specific technology examples within the Implementation Guidance, much like was presented at the March 3, 2021 Webinar.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment
GSOC agrees that the requirement fulfills the directive and respectfully suggests the following clarifications: 1. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion. 2. Clarification of the included exclusions is recommended as follows: …excluding data being transmitted between Control Centers that is subject to CIP-012 and time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment
We recognize that the SDT has realigned the requirement to protect nonprogrammable communication components from CIP-006 R1 to CIP-005 R1. As CIP-006 R1 previously addressed Order 791 Paragraph 150, we feel CIP-005 R1 continues to address the identified gap.

Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	Yes
Document Name	

Comment
Change follows FERC Order 791, however, reference to the CIP-012 standard and the addition of a specific protocol in the requirements area should be removed and placed into the measures area.

Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
The proposed requirement appears to meet the directive in FERC Order 791, paragraph 150. However, the proposed applicability of this requirement significantly expands the scope from CIP-006 R1.10 that focuses on Control Centers to high/medium BES Cyber Systems, PCAs, PACS, and EACMS. This revision appears to be beyond the scope of the SDT's SAR.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
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	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
Teresa Cantwell - Lower Colorado River Authority - 5	

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	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 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	
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	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
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	

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	

5. The SDT modified CIP-005 Requirement R2 to ensure remote access management requirements align with the new and revised virtualization terms. Do you agree with the proposed changes? 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	
Clarify the definition of "system to system" in Parts 2.4 and 2.5 to provide consistent application of the standard.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
1. As SRP reads, R2.1: “Ensure…” should be replaced with strong verbiage. R2.2: “Protect the confidentiality and integrity…” appears to provide flexibility, it will likely result in entities seeking and following the opinion of auditors on what is sufficient. SRP would prefer 2.2 be the first requirement in the R2 section, then 2.1 and 2.3.	
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: In order to accommodate the SDT language for these requirements, the definition of IRA could be revised per our recommendations in Question 1 to include routable connectivity for the initiation of Interactive Remote Access.	

Recommendations:

- Retain the current CIP-005-6 R2 language and revise the Applicable Systems to change from Medium Impact with ERC to Medium Impact with IRA.
- Retain the current CIP-005-6 R3 language for Applicable Systems.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

The proposed definition and requirements decouple ERC as a qualifier for IRA and imposes additional requirements on systems that were previously out of scope. This prevents backwards compatibility for entities with serial connections to medium impact BCS at substations and generation facilities. The requirement was modified to address conversion from IP to serial protocol conversion at a substation or generating facility due to the perceived risk of the routable communications. However, the changes adversely impact entities that use the “500 mile serial cable” for communications. How does an entity protect confidentiality and integrity of communications on a serial link that transverses through an asset boundary? The proposed revisions ultimately require the conversion of substations/facilities with serial connections to BCS with ERC in order to meet IRA requirements in CIP-005 R2.

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

Comments: In order to accommodate the SDT language for these requirements, the definition of IRA could be revised per our recommendations in Question 1 to include routable connectivity for the initiation of Interactive Remote Access.

Recommendations:

- Retain the current CIP-005-6 R2 language and revise the Applicable Systems to change from Medium Impact with ERC to Medium Impact with IRA.

Retain the current CIP-005-6 R3 language for Applicable Systems.

Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	No
Document Name	

Comment

An entity may find the wording confusing. It could be read as only communication to another Intermediate System is permitted. In addition, in this case, recommend changing the term “Intermediate System” to “EACMS used to restrict IRA”.

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

Answer	No
Document Name	

Comment

The proposed language greatly expands scope of this requirement by adding PACS and EACMS, which were not previously in scope.

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

For CIP-005 Requirement R2.1, ISO-NE recommends the replacement of the word “ensure” as this represents internal control language and is inconsistent with all other requirements. ISO-NE suggests the following replacement language:

“For all IRA, utilize an Intermediate System (IS).”

For CIP-005 Requirement R2.2, ISO-NE recommends removal of the cross-reference to another Part of the same requirement in the Applicable Systems, “Intermediate Systems used to access applicable systems of Part 2.1.” This approach deviates from other CIP “Applicable Systems” columns and requires a reader to refer to other requirements for scope. ISO-NE suggests either including the CIP-005 Part 2.2 requirements in the CIP-005 Part 2.1 requirements, or adjusting CIP-005 Part 2.2 to state “Intermediate Systems used for IRA.”

For CIP-005 Requirement R2.3, ISO-NE recommends removal of the cross-reference to another Part of the same requirement in the applicable systems, “Intermediate Systems used to access applicable systems of Part 2.1.” This approach deviates from other CIP “Applicable Systems” columns and requires a reader to refer to other requirements for scope. ISO-NE recommends adjusting CIP-005 Part 2.3 to state “Intermediate Systems used for IRA.”

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 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 does not support the proposed changes to R2 and requests that the SDT consider the following comments:

• Southern requests that the SDT consider that the R2.1 requirement, as currently proposed, (1) adds further scope expansion from previous versions, and (2) reintroduces again the concept of the “Hall of Mirrors” where the object of the requirement (an EACMS-Intermediate System) is also an Applicable System (EACMS) where the object must apply the requirement to itself.

o In the first case, PACS assets have historically not been required to have an EACMS-Intermediate System regulate remote access to them; here PACS hosted on SCI have been added as an Applicable System, which now would require an entity implement an EACMS-IS for remote access to PACS assets hosted on SCI, and the IRA definition has been expanded to now make IRA applicable to PACS assets hosted on SCI because IRA is no longer tied to the outer boundary of an “ESP”.

o In the second case, the Applicable Systems column includes EACMS hosted on SCI, which now requires that IRA to an EACMS go through an Intermediate System; however, the Intermediate System is also an EACMS and IRA to it would therefore require another Intermediate System in front of it, and so on and so forth.

o However, a review of the revised definition of EACMS states:

 Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of **the logical isolation of BES Cyber Systems.** This includes Intermediate Systems.

 This definition of an EACMS explicity excludes itself from performing electronic access controls (IRA) or electronic access monitoring for PACS assets or other EACMS assets, whether hosted on SCI or not, and rather only includes that performance for the "***logical isolation*** of BES Cyber Systems", and not PACS, other EACMS, or the BES Cyber Systems themselves.

• It is also not explicitly clear what is meant by the term "from outside of the asset containing the system being accessed" from the IRA definition. Southern recommends the SDT provides clarification on this specificity in defining IRA that appears to make any communication from outside of the "asset" (little "a", Facility) where the system being accessed "resides" as now being IRA. This seems ot be a result of the concepts of losing the outer boundary of an ESP such that the definition of "remote" becomes very broad. As a result, for those entities that do retain ESPs as a form of Logical Isolation, this significantly complicates inter-ESP communication that spans multiple "assets" or Facilities.

• Under Requirement R2.6.1, the requirement is written in a way that could be interpreted to mean that all Intermediate Systems must be virtualized and therefore must, in every case, only "share CPU and memory with other Intermediate Systems and their associated SCI." Southern requests the SDT consider the addition of the following phrase to the requirement as follows: "Restrict Intermediate Systems ***hosted on SCI*** to only share CPU and memory with other Intermediate Systems and their associated SCI."

o Additionally, the R2.6.1 language confirms the interpretation that Intermediate Systems hosted on SCI and associated with any of the Applicable Systems from Part 2.1 cannot share virtual space or Management Systems with BES Cyber Systems or non-CIP assets, and therefore must be stand-alone systems. A utility is then required to have at least three separate sets of hardware/management systems: one for medium and high BCS, one for IS, and one for associated PACS and EACMS hosted on SCI (and more if using virtualization for non-CIP/exempt cyber assets and/or separating medium impact and high impact assets from a risk-based perspective). This seems to disincentivize the use of, and achievement of better security offered by, virtualized systems and architectures.

• The Technical Rationale for CIP-005-8 mentions that this is now an objective-based requirement, but that outdated encryption methods or protocols would not meet the objective. Who decides what encryption methods or protocols are "outdated" and thus would be non-compliant? Can a list of these be provided by NERC and the Regions? Can the SDT remove this from the TR and potentially allow common sense to apply to appropriate security and encryption protocols between entities and auditors?

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

RF does not agree with the proposed changes for the following reasons:

A significant concern is that an entity could implement logical isolation using only a host-based firewall and essential systems could be directly connected to the internet – a side effect breaking the definition of External Routable Connectivity and enabling entities to bypass many now-required protections.

With each system becoming its own ESP (zero trust) – mixing of CIP and non-CIP network traffic is permitted and could lead to issues regarding secure communications if implemented policies are not closely scrutinized and exceptional care taken to maintain and control policies on each individual Cyber Asset.

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.

Logical Isolation is not defined, leading to diverse definitions between the entities and regions.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

R2.1: The Intermediate System is an EACMS. Adding associated EACMS to the Applicable Systems creates an EACMS for an EACMS situation. There is no need for this requirement to be applicable to associated PACS or EACMS. The Intermediate System is designed to protect IRA sessions to logically isolated systems. If any PACS or EACMS are inside the logical isolations, then those PACS or EACMS are PCAs. We recommend removing “PACS or EACMS” from the Applicable Systems for both SCI and Management Modules.

R2.2: We understand the concept of the requirement as currently written, “ For all IRA sessions, utilize encryption that terminates at the Intermediate System.” The revised language “between the client and the Intermediate System” is not clear. Either clarify or define “the client” in the requirement or revert back to the current language.

R2.6: Is the intent to require any virtualized Intermediate System(s) to be hosted on SCI that does not contain virtual BCS, EACMS, PACS or PCAs? Please clarify the intent.

R2.6.2 seems duplicative of R1.1. R2 requires Intermediate Systems to be used to access logically isolated applicable systems. R1.1 requires that we identify needed communications. If the communications between the Intermediate Systems is needed and controlled into the logically isolated systems, then R2.6.2 is redundant and covered by R1.1. Please clarify the SDT intent for R2.6.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Could you please specify the kind of access you are referring to for IRA? For example, we have operators that will issue commands to close or open a breaker, start or shutdown a Turbine generating unit. But they don't have access to configure or change the configuration of the asset. In that case is that consider IRA ? Our understanding is that the "User-initiated access by a person employing a remote access client" you are referring to, is basically **for configuration changes** from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed. Proposed definition: User-initiated access by a person employing a remote access client from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed; **excluding control functions** (e.g. access for issuing commands)	
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

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 standard requires that an entity must use an IS to access and EACMS but and IS is an EACMS so do you need and IS to access and IS? This comment is based on the interpretation by some SMEs that CIP-005 R2.1 includes with IRA including the VCA hosted by them (discussed below).

In requirement 2.1 for:

SCI with IRA hosting High or Medium Impact BCS or their associated:

PCA

PACS; or

EACMS

For R2.1 It is not clear if EACMS and PACS on SCI is applicable if there is no High or Medium Impact BCS on the same SCI. Some SMEs read that EACMS and PACS are only applicable if High or Medium Impact BCS are on the same SCI; other SMEs read the applicability to be associated EACMS and PACS on SCI, regardless of whether the High or Medium Impact BCS are virtual. A third way to interpret the applicability is that SCI with IRA hosting high or medium impact BCS or associated PCA, PACS or EACMS must have an intermediates system just to access the manament system. It's unclear what the applicable systems are.

For CIP-005 R2 and others, where the intent may be to protect the SCI or have the SCI be the applicable system, it might be better to write like this:

SCI with IRA hosting:

High or Medium Impact BCS or their associated;

PCA;

PACS; or

EACMS

The above would make it clear that the applicable system is the SCI.

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	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
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	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
R2.1: The Intermediate System is an EACMS. Adding associated EACMS to the Applicable Systems creates an EACMS for an EACMS situation. There is no need for this requirement to be applicable to associated PACS or EACMS. The Intermediate System is designed to protect IRA sessions to logically isolated systems. If any PACS or EACMS are inside the logical isolations, then those PACS or EACMS are PCAs. We recommend removing “PACSor EACMS” from the Applicable Systems for both SCI and Management Modules.	

R2.2: We understand the concept of the requirement as currently written, “For all IRA sessions, utilize encryption that terminates at the Intermediate System”. The revised language “between the client and the Intermediate System” is not clear. Either clarify or define “the client” in the requirement or revert back to the current language.

R2.6: Is the intent to require any virtualized Intermediate System(s) to be hosted on SCI that does not contain virtual BCS, EACMS, PACS or PCAs? Please clarify the intent.

R2.6.2 seems duplicative of R1.1. R2 requires Intermediate Systems to be used to access logically isolated applicable systems. R1.1 requires that we identify needed communications. If the communications between the IS is needed and controlled into the logically isolated systems, then R2.6.2 is redundant and covered by R1.1. Please clarify SDT intent for R2.6

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CHPD does not agree with the CPU and memory isolation requirements. In particular, it prevents other potential mitigations, such as non-persistent Intermediate Systems where malware would be unable to gain a foothold, and unduly increases the cost of virtualization. See comments for question 19.

“(e.g., encryption)” in CIP-005 R2.2 should be moved to Measures.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Request clarification on R2.1 “ensure.” The requirement says “Ensure that IRA is through an Intermediate System.”

Request clarification on the definition of SCI (including Management Systems) and the column applicable systems, in requirement 2.1 Management Modules

Suggest not to include PACS and EACMS in the scope in the context of SCI as this requirement doesn't exist for a PACS and EACMS not on a SCI.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Additional clarity is needed on the new terms to see how this requirement affects an entity's facility that contain Medium Impact BCS.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	

Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
The definition of IRA would need to be reviesed to include routable connectivity for the initation of Interactive Remote Access.	
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 CIP-005 Requirement R2 due to the proposed IRA definition. Please see response to Question 1 for additional details.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
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 CIP-005 Requirement R2 due to the proposed IRA definition. Please see response to Question 1 for additional details.

Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	

AEP is concerned that proposed changes to CIP-005 Requirement R2 may have created some unintended gaps in how the requirements may be audited and seeks additional clarification. AEP fully supports EEI's suggestions, copied below for reference.

Part 2.1: Requirements do not specify that the Intermediate Systems (IS) must be logically separated from the system being accessed. The current IS definition states that it must be located outside the ESP. The Technical Rationale for the IS definition states that placement of IS has been moved to R2. AEP seeks clarification on how this is addressed within Requirement R2.

Part 2.2: The proposed IRA definition states that IRA shall be from outside the logical isolation of the system being accessed. R2, Part 2.2 requires that IRA between client and IS must be protected. Assuming the client is the initiating device, there must be logical separation between client and IS. Considering this and what was previously required, separation was required between IS and BCA (i.e., "IS must be outside ESP"). AEP's concern with R2, Part 2.2 is that it is no longer clear if that level of isolation is still required. The existing requirement should be clarified to address what is required.

- Clarification is needed on the change from "encryption that terminates at an intermediate system" to "between client and the IS". It is not clear where encryption is required. Diagrams in the Technical Rationale would be useful to ensure that entities understand what is expected.
- We also note that the Technical Rationale states that R2, Part 2.2 is now objective-based and the requirement now "prevents outdated encryption methods from being used that no longer meet the objective." (CIP-005-8 Technical Rationale, R2, Part 2.2, page 10). Clarification is needed on who makes this determination and how this would be determined.

Part 2.6: AEP also suggests to add Applicable Systems from Part 2.1 to Part 2.6 instead of just referencing it.

- Part 2.6.1: Is this intended to separate IS from exempt cyber assets, meaning IS cannot be hosted by Management Systems shared with non-CIP systems? This also prevents IS from being hosted by Management Systems containing BCS. The result is that, in a virtualized environment, a utility requires three separate sets of hardware/management systems: one for medium and high BCS, one for IS, and one for non-CIP/exempt cyber assets. Can IS be hosted on SCI with non-CIP systems? Again, the "IS" definition in the glossary indicates IS placement is handled in CIP-005 R2 but that detail is not included here.

- Part 2.6.2: AEP is concerned that this requirement may be duplicative of Requirement R1, Part 1.1. In Part 1.1, it already requires that EACMS "Permit only needed and controlled communications to and from applicable systems" and the IS definition indicates it is a "type of EACMS". For these reasons, Clarification is needed on why R2, Part 2.6.2 is not duplicative to R1, Part 1.1.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

AEPCO is signing on to ACES comments, please see below:

ACES does not agree with the language used in requirement R2.2. "Client" is a vague and an undefined term. We suggest:

Protect the confidentiality and integrity (e.g., encryption) of IRA between the remote host and the Intermediate System.

ACES does not agree with the language used in R2.6.2 as it is redundant to R1.1 and not necessary. If implemented, any communications with Applicable Systems in part 1.1 would already be permitted, controlled, and documented, which would include IRA, and make R2.6.2 unnecessary. If the scope of R1.1 does not include all of R2.1, updating the scope of R1.1 would suffice.

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

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
CIP-005, R2.2 does not clearly define what a “client” would be in reference to encryption between the client and the Intermediate System. Additional clarity is necessary to ensure consistent application of the proposed Standard.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren generally agrees with EEI's comments with some added suggestions. We suggest that the SDT include examples of remote access that include a virtualized desktop environment. We also suggest that the IRA definition should say you cannot have IRA from another cyber asset.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
“Ensure that authorized IRA is through an Intermediate System. “ – Can we communicate through the firewall? Previous standard was accurate. New standard is subjective and will create confusion.	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
The term “ensure” is unclear. How will this be interpreted by regions and auditors? This needs to be clarified	
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	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
R2.2 and 2.3: With the revised definition, it is unclear if Intermediate System, defined as “An Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access”, is referring to a jump host or an authentication system. Based on the language used, encryption is only required during the authentication phase. R2.4: The language states that a method for determining active vendor remote sessions is required. However, the measures appear to be primarily focusing on logging of access while ignoring real time access. Is the intent to log, or is the intent to be able to identify active sessions. Intent and language in the requirement is unclear.	
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 language used in requirement R2.2. “Client” is a vague and an undefined term. We suggest: Protect the confidentiality and integrity (e.g., encryption) of IRA between the remote host and the Intermediate System. ACES does not agree with the language used in R2.6.2 as it is redundant to R1.1 and not necessary. If implemented, any communications with Applicable Systems in part 1.1 would already be permitted, controlled, and documented, which would include IRA, and make R2.6.2 unnecessary. If the scope of R1.1 does not include all of R2.1, updating the scope of R1.1 would suffice.	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
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	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
DTE sees the applicability for R2, as described in the R2 description, to be inconsistent and potentially confusing and recommends that the applicability, "For all remote access that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs", be moved to the "Applicable Systems" section in some manner to avoid this confusion.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP offers the following comment for the SDT consideration for Question 5: Recommend the SDT consider R2.6 be written in the definition, or considered in CIP-002.	
Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-005, R2. PG&E does have concerns and supports the input provided by EEI.	
Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
R2.1: The Intermediate System is an EACMS. Adding associated EACMS to the Applicable Systems creates an EACMS for an EACMS situation. There is no need for this requirement to be applicable to associated PACS or EACMS. The Intermediate System is designed to protect IRA sessions to logically isolated systems. If any PACS or EACMS are inside the logical isolations, then those PACS or EACMS are PCAs. We recommend removing “PACSor EACMS” from the Applicable Systems for both SCI and Management Modules. R2.2: We understand the concept of the requirement as currently written, “For all IRA sessions, utilize encryption that terminates at the Intermediate System”. The revised language “between the client and the Intermediate System” is not clear. Either clarify or define “the client” in the requirement or revert back to the current language. R2.6: Is the intent to require any virtualized Intermediate System(s) to be hosted on SCI that does not contain virtual BCS, EACMS, PACS or PCAs? Please clarify the intent. R2.6.2 seems duplicative of R1.1. R2 requires Intermediate Systems to be used to access logically isolated applicable systems. R1.1 requires that we identify needed communications. If the communications between the IS is needed and controlled into the logically isolated systems, then R2.6.2 is redundant and covered by R1.1. Please clarify SDT intent for R2.6	
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 R2.1 “ensure.” The requirement says “Ensure that IRA is through an Intermediate System.”

Request clarification on R2.1 “ensure.” The requirement says “Ensure that IRA is through an Intermediate System.”

Request clarification on the definition of SCI (including Management Systems) and the column applicable systems, in requirement 2.1 Management Modules.

Suggest not to include PACS and EACMS into the scope in the context of SCI as this requirement doesn’t exist for a PACS and EACMS not on an SCI.

Likes 0	
Dislikes 0	
Response	

Douglas Webb - Douglas Webb 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; - Douglas Webb

Answer	No
Document Name	
Comment	

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 5.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

Requirement R2

2.1: Requirements do not specify that the Intermediate Systems (IS) must be logically separated from the system being accessed. The current IS definition states that it must be located outside the ESP. The Technical Rationale for the IS definition states that placement of IS has been moved to R2. EEI seeks clarification on how this is addressed within Requirement R2.

2.2: The proposed IRA definition states that IRA shall be from outside the logical isolation of the system being accessed. R2, Part 2.2 requires that IRA between client and IS must be protected. Assuming the client is the initiating device, there must be logical separation between client and IS. Considering this and what was previously required, separation was required between IS and BCA (i.e., "IS must be outside ESP"). EEI's concern with R2, Part 2.2 is that it is no longer clear if that level of isolation is still required. The existing requirement should be clarified to address what is required.

EEI also seek clarification on the change from "encryption that terminates at an intermediate system" to "between client and the IS". It is not clear where encryption is required. Diagrams in the Technical Rationale would be useful to ensure that entities understand what is expected.

We also note that the Technical Rationale states that R2, Part 2.2 is now objective-based and the requirement "prevents outdated encryption methods from being used that no longer meet the objective." (CIP-005-8 Technical Rational, R2, Part 2.2, page 10). EEI requests clarification on who makes this determination and how this would be determined.

2.6.1: Is this intended to separate IS from exempt cyber assets, meaning IS cannot be hosted by management systems shared with non-CIP systems? This also prevents IS from being hosted by management systems containing BCS. The result is that, in a virtualized environment, a utility requires three separate sets of hardware/management systems: one for medium and high BCS, one for IS, and one for non-CIP/exempt cyber assets. Can IS be hosted on SCI with non-CIP systems? Again, the "IS" definition in the glossary indicates IS placement is handled in CIP-005 R2 but that detail is not included here.

2.6.2: EEI is concerned that this requirement may be duplicative of Requirement R1, Part 1.1. In R1, Part 1.1 it already requires that EACMS "Permit only needed and controlled communications to and from applicable systems" and the IS definition indicates it is a "type of EACMS". For these reasons, EEI requests clarification why R2, Part 2.6.2 is not duplicative to R1, Part 1.1.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	No
Document Name	

Comment

In R2 there is a Hall of Mirrors effect. In R2.1 it appears the EACMS on SCI needs to have IRA through an Intermediate System, but an Intermediate System itself is by definition an EACMS. So if I have my Intermediate System on SCI then does that Intermediate System which is a EACMS on SCI also need another Intermediate System to perform IRA?

We have a concern about R2.6. Many multifactor authentication systems reside on the domain controller. The Multifactor authentication is part of the Intermediate System. The concern is restricting the sharing of CPU and memory. These domain controllers may also be EACMS for other devices. Can we restrict the sharing of CPU and memory to other in scope CIP devices to allow more flexibility in architecture?

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	
Comment	
Request clarification on R2.1 “ensure.” The requirement says “Ensure that IRA is through an Intermediate System.”	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
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 that as presently drafted, CIP-005 R2 and CIP-005 R3 conflict with one another. Please see our explanation and recommendations for resolving this problem in our response to Question 19.	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	

Comment
We don’t agree with replacing ERC with IRA, as it will bring into compliance more devices that were previously excluded. Additionally, we recommend that R2.4 – 2.5 are updated with the same exclusion as R1.3 for Real-time Assessment and real-time monitoring data. We do not believe ICCP protocol should be considered vendor system-to-system remote access. Our EMS system does not allow modifications through the ICCP protocol, thus there is no “access”.

Likes 0	
Dislikes 0	

Response

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

Comment
The standard should contemplate the use of encryption and multifactor between the Intermediate System and the Cyber Assets within the ESP. As written, it appears to prohibit that. ERCOT suggests that the Part 2.2 example should be in the measure.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	

Comment
Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Part 2.6.2 security objective appears to already be addressed in Part 1.1.	
Likes 0	

Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the proposed modifications, but has identified concerns with the impact of anti-affinity rules as described in the general comments below.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Reclamation recommends having a documented process for approving vendor remote access sessions through a change control board.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes this effectively expands the scope of the control by including serial only devices that allow interactive remote access via a serial to Ethernet converter. Guidance needs to make clear how an entity would comply with requirements intended for Ethernet protocols when using interactive remote access over serial connections.	
Likes 0	

Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments regarding the proposed revisions to CIP-005, requirement R2:

3. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

4. In the applicable systems column, ERC has been struck with respect to Medium Impact BCS and IRA or vendor remote access has been added. This is different from other areas where IRA has been added to a similar requirement and ERC has been retained and vice versa. While it is understood that such scoping can better tailor the requirements, inconsistent application and use of scoping verbiage can lead to ambiguity and confusion. For this reason, review and use of consistent scoping verbiage is recommended.

5. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column in R2 and R3 references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

6. The intent and expectations of requirement R2.1 is unclear. As revised, the new requirement could be construed as allowing the Intermediate System to acts as a pass-through or flow-through device that is not contributing to the security controls applied to IRA. Suggest clarification through the proposed revisions below:

Ensure that IRA is [implemented/controlled] through an Intermediate System.

7. CIP-004 does not address the authorization of electronic access to Management Modules; however, requirements in Requirement R2.1 hint that there are expectations and obligations associated with access to these assets. This should be clarified.

8. In requirement R2.6, the following revision is recommended for clarity:

2.6.2. Permit only controlled communications that are [needed/necessary] between Intermediate Systems and applicable systems of Part 2.1.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes.	
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 requests clarification from the SDT regarding “confidentiality and integrity” controls and what encryption methodologies would serve the Requirement. This clarification could be contained in the CIP-005 Implementation Guidance describing message integrity provided by application layer encryption like HTTPS & TLS.	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	Yes
Document Name	
Comment	
For purposes of our response to question 5, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO and PJM.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Likes 0	

Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 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	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 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	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	

Comment	
Exelon is aligning with EEI in response to this question.	
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	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	

Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

6. The SDT revised CIP-007 Requirement R1 Part 1.1 to shift the security objective from logical network accessible ports to services. The proposed revisions require Responsible Entities to enable only network accessible services that have been determined to be needed by the Responsible Entity. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

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

As written, CIP-007, R1, Part 1.1 continues to reference both ports and services:

- Requirement: “Enable only network accessible services that have been determined to be needed…, or the logical network accessible *ports* if unable to determine service, including *port* ranges where needed to handle dynamic *ports*) per system capability”
- Measure: “Documentation of the need for all enabled *ports*.”

Recommendation: If the intent is to focus on services only, the SDT should clarify this in non-ambigous terms; i.e. indicate entities will be audited on "**services only**" (as opposed to "*ports and* services").

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Please see comments submitted by the ISO/RTO Council Standards Review Committee.

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

Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	No
Document Name	
Comment	
PNMR expresses support of comments by Joshua Andersen, On Behalf of: Salt River Project, WECC, Segments 1, 3, 5, 6	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
What is the value of removing ports if the phrase “(or logical ports)” is added every time services is used?	
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

General comment on CIP-007. Request consistent use of “system hardening.” We concerned that the label “system hardening” is used differently in the R3.1 Measures and with Transient Cyber Assets.

Request clarification of “services” – entity may need to map their BES Cyber Assets to Applicable Systems.

Suggest reviewing the Requirements column for requirements 1.1 and 1.3, the objective is the same, yet the text isn’t. It should have the same level of detail.

Suggest reviewing the Applicable Systems of CIP-007 should include Management Systems.

Suggest not to include PACS and EACMS into the scope in the context of SCI as this requirement doesn’t exist for a PACS and EACMS, not on an SCI. SAR is for including the virilization concepts not to add additional controls.

Suggest reviewing the Applicable Systems of CIP-007 associated with management modules. The current language only refers to Management Modules of SCI hosting what about the management module of a BCA? Management Modules of SCI hosting would have more controls than Management Modules of BCA.

Request clarification on the term system (cybersecurity patches for systems), the objective is for the system to be patched or for the cyber asset composing the system to be patched?

Request clarification on the term system capability (Log security events, per system capability), logging from one cyber asset would be enough to comply with the requirement?

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 SRC and requests additional clarity on the use of the term “enable”. Is the term intended to “allow” or “restrict” network accessible services and should the term be adjusted as such?

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We agree with the proposal; however, please update the measures to match. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP offers the following comment for the SDT consideration for Question 6: Recommend the SDT change the word “ports” to the word “services” in the measure, as the requirement was changed to focus on the standards.	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Referring to the Change Rationale for CIP-007 Part 1.1, DTE recognizes the clear direction shift from "ports" to "services". However, R1.1 infers that a port listing may still be required to justify the service. The “Measures” does not reference “services”. DTE would recommend additional measures that demonstrate potential compliance strategies that do not require the demonstration of “ports”. Without such reference it may be inferred that such a “port” list is a prescriptive requirement, which would not provide any relief to the entity's burden of compliance.	
Likes 0	

Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	

Comment
Concerns on the definitions caused this no vote for this standard. The change the requirement title to "System Hardening" is unclear. "System hardening" is used in section 3.1 as an alternative to AV and as part of the TCA/RM requirements. The TR states, "harden the applicable systems through limiting access to logical services and physical ports" but the requirement language states "Services and logical ports."

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	

Comment
FMPA supports Marty Hostler and Northern California Power Agency comments.

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
Services are typically associated with Cyber Assets running an operating system. There is no technical or risk basis for changing from ports to services. While an open port is associated with a running process (service), on firmware based Cyber Assets and some software appliances, they do

not have the ability to discern the running process (service) which the port is open. Further, part of the attack surface of a Cyber Asset is determined by its open ports. Processes may or may not be discernable. Network accessible ports are consistent across any platform running a TCP stack and can be determined easily. While the new language in the requirement allows for documenting ports as a secondary mechanism, there is not technical merit or risk reduction in documenting services over network accessible ports. This also was not a part of the FERC order or SAR.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	

Comment

A requirement to control logical ports makes far more sense than services. If services is the term used, services needs to become a defined term. There are many ways to interpret the term services. Windows and Linux each have different approaches to managing and using the term services. Application frameworks use the term differently as well.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

The revision to CIP-007 Requirement Part 1.1 needs to be clarified. The “or” statement will cause different interpretations across regions and auditors.

The proposed use of “system hardening” in CIP-007 is inconsistent and not defined

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment
Unnecessary confusion. Previous standard language was sufficient for design of security controls and application. Revert to old standard, which industry has worked hard to standardize and create controls that have been effective.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
R1.2 - Additional clarification is needed to clearly determine what the term “non-programable communications components” means. R2.1 – As written, it appears that patching can be performed at the “system” level vs at the individual CA level. Additional language should be added to clarify the intent of the team as the current language is ambiguous. R4.1 – As written, it appears that logging should now be performed only at the system level and does not allow for additional logging at the CA level. Additional language should be added to clarify the intent of the team as the current language is ambiguous.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
AEPCO is signing on to ACES comments, please see below: Services are typically associated with Cyber Assets running an operating system. There is no technical or risk basis for changing from ports to services. While an open port is associated with a running process (service), on firmware based Cyber Assets and some software appliances, they do not have the ability to discern the running process (service) which the port is open. Further, part of the attack surface of a Cyber Asset is determined by its open ports. Processes may or may not be discernable. Network accessible ports are consistent across any platform running a TCP stack and can be determined easily. While the new language in the requirement allows for documenting ports as a secondary mechanism, there is not technical merit or risk reduction in documenting services over network accessible ports. This also was not a part of the FERC order or SAR.

Likes 0	

Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
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 Measures section of CIP-007 Requirement R1 Part 1.1. The STD should update the Measures to include the “listing of services” instead of keeping the existing “ports” language since it is not consistent with the changes to the Requirement language.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE 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 changes to the Measures section of CIP-007 Requirement R1 Part 1.1. The STD should update the Measures to include the “listing of services” instead of keeping the existing “ports” language since it is not consistent with the changes to the Requirement language.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
More clarity is needed for the change to this requirement. Are there examples as to where there would be a network accessible service without an associated network accessible port?	
Likes 0	

Dislikes 0	

Response

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

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Suggest reviewing the applicable systems column should include SCI hosting High or Medium Impact BCS or their associated: PCA

Suggest reviewing the Requirements column for requirements 1.1 and 1.3, the objective is the same, yet the text isn't. It should have the same level of detail.

Suggest reviewing the Applicable Systems of CIP-007, should include Management Systems.

Suggest not to include PACS and EACMS into the scope in the context of SCI as this requirement doesn't exist for a PACS and EACMS not on a SCI. SAR is intended for virilization concepts, not to add additional controls.

Suggest reviewing the Applicable Systems of CIP-007 associated to management modules. The current langage only refers to a Management Modules of SCI hosting . What about a the management module of a BCA ? Management Modules of SCI hosting would have more controls than a Management Modules of BCA.

Request clarification on the term "system" (cyber security patches for systems). Is the objective for the system to be patched or for the cyber asset composing the system to be patched ?

Request clarification on the term system capability (Log security events, per system capability), logging from one cyber asset would be enough to comply with the requirement ?

Likes 0	
Dislikes 0	

Response

Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	No
Document Name	

Comment

Entergy cannot support this standard as written due to a lack of clarity regarding required documentation and adequate information to inform expected auditing approach. The standard states "or logical network accessible ports if unable to determine service" but the Requirements and the Measures, as well as the lack of a Guidelines & Technical Basis section, do not provide adequate guidance on what documentation is expected to enable only logical network accessible ports as

opposed to services. If an entity identifies that they are “unable to determine service”, what evidence, if any, would be required by the entity to justify the inability to determine service?

Additionally, although the Requirement has been changed to shift the focus from ports to services, the measures as written still focus on the documentation of ports and makes no mention of services, which leads to ambiguity for the entities on how to achieve compliance.

The SDT is recommended to provide additional clarity regarding evidenciary examples for a.) when the entity is unable to determine service and is instead limiting ports; and b.) update the measures to provide clarity on examples of evidence related to services and/or ports.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with the proposal; however, please update the measures to match.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Part 1.1: Changes focus from ports to services, requiring enabling only needed services. Entity may fall back on port identification only when services cannot be identified. The shift to focusing on looking at services could restrict auditor visibility in the case where a service arbitrarily uses overly large port ranges. The part does include the language “including port ranges where needed to handle dynamic ports” however this would result in the auditor not knowing the port ranges associated with all services deemed necessary. The onus would then be put on the auditor to determine the ports associated with a particular service and whether the port ranges are reasonable or not. In addition, entities focus would be on authorized services and not on the actual system vulnerability of an increased attack surfaced created by ports that are not intentionally disabled. A recommended change may be “Disable all logical network accessible ports except those associated with network accessible services that have been determined to be needed by the Responsible Entity (or logical network accessible ports if unable to determine service, including port ranges where needed to handle dynamic ports), per system capability. If a system has no provision for disabling or restricting network accessible services (or logical ports) then those services (or logical ports), that are open are deemed needed.”	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
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 finds the following requirement language unclear, "…network accessible services (or logical ports), that are open are deemed needed." The language seems subjective and may be interpreted to mean 'can be open' or 'open for a period of time' which presents a compliance risk. For this reason, ISO-NE recommends defining network accessible services.

Additionally, CIP-007 Part 1.3 conflicts with Part 1.1, both parts should be combined because virtual hosts and physical hosts would run on the same ports. The physical attribute is the only aspect addressing ports; the distinction between virtual vs. physical adds confusion.

ISO-NE appreciates the removal of TFEs and understands that system capability requirements are still in place and will need to be documented.

Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	No
Document Name	

Comment

We agree that a focus on services is warranted, however entities will need clarification of the term "services" to correctly scope their CIP programs.

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

Comments: We recommend revising SDT's proposed language.

Recommendation:

- Revise the current CIP-007-6 language to read:

"Enable only logical network accessible ports or services determined to be needed by the Responsible Entity per system capability. If an applicable Cyber Asset or BCS has no provision for disabling or restricting network accessible ports or services on the Cyber Asset or BCS, then those open ports or services are deemed needed."

Likes 0	

Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

Please consider the following proposed requirement, “The Responsible Entity shall determine which network accessible services are needed and enable only those services (or logical network accessible ports if the Responsible Entity is unable to determine the service, including ports ranges where needed to handle dynamic ports), per system capability. If a system has no provision for disabling or restricting network accessible services (or logical ports) then those services (or logical ports) that are open are deemed needed.”

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: We recommend revising SDT’s proposed language.

Recommendation:

- Revise the current CIP-007-6 language to read:

“Enable only logical network accessible ports or services determined to be needed by the Responsible Entity per system capability. If an applicable Cyber Asset or BCS has no provision for disabling or restricting network accessible ports or services on the Cyber Asset or BCS, then those open ports or services are deemed needed.”

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
1. SRP request clarification with the concept “If a system has no provision for disabling or restricting network accessible services (or logical ports) then those services (or logical ports), that are open are deemed needed.” 2. Is this requirement addressing just vitural environements or can the physical environment (current) version also be part of this new requirement. SRP has questions concerning backward compartible if we are not in a virtual environment. Or is this requirement speaking only to virtualization, and if this is the case - physical would have to be backward compatibility. 3. What is the value of removing ports if the phrase “(or logical ports)” is added every time services is used?

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
Revise to clarify that only "listening ports" are the subject of the requirement. The proposed language does not differentiate between established and listening ports.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	
Comment	
EEI supports the proposed shift from logical network accessible ports to services.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 6.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the approach for CIP-007, R1, Part 1.1.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes

Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE agrees with the proposed changes to CIP-007. Texas RE recommends, however, clarity be provided on the term “network accessible services”. While the measure mentions listening ports, there is no language in the requirement clarifying network accessible services.	
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	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

Ameren agrees with and supports EEI's comments.	
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	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
LCRA supports this change.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the proposed shift from logical network accessible ports to services.	

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
LCRA supports this change.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS would like for a clearer definition of what a “service” entails.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
The change does not seem to pose any concerns from ports to services. There still continues to be a disconnect from CIP-007 R1.1 and CIP-010 R1.1. Is there a fundamental reason why CIP-007 R1.1 applies to Medium Impact systems that have ERC but the baselines requirements of CIP-010 R1.1 apply to all Medium Impact systems? Those two sub-requirements seem like they should sync up one way or the other.	
Likes 0	

Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
While CHPD does not disagree with this change, it seems to be unnecessary as CIP-007 R1.1 already requires the entity to demonstrate the need for the port. In doing so, the entity indirectly documents the service by explaining the need for the port.	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC provides the following comments for the SDT’s review and consideration: 9. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.	

10. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

No comments

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment	
We agree with the proposal; however, please update the measures to match.	
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	
Yes, Southern supports these proposed revisions to shift the security objective to enabled services. Southern also requests that the SDT remove the phrase “per system capability” (along with “Where technically feasible”). The second sentence of R1.1 states that where a system has no provision for … which covers an entity in all situations and therefore a TFE or a “per system capability” exemption is not needed. Additionally, Southern requests the SDT consider the potential for “double jeopardy” with regulators with regard to CIP-007 R1 and CIP-010 R1 when providing evidence to support compliance for enabled services. Any failure to authorize and document changes to services as per CIP-010 R1 can also result in a potential violation of CIP-007 R1 as services may be enabled without documented authorization; Southern requests the SDT consider modifications to eliminate the duplicative nature of the two requirements and remove the potential for double jeopardy.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
THE SELECTION SHOULD BE NO TO THE QUESTION.. THE SBS SYSTEM WILL NOT ALLOW FOR EDITS AFTER A SELECTION HAS BEEN SAVED. Duke Energy agrees with the intent of a services based approach but does not agree with the revision as worded. Duke seeks clarification that entities may credit existing port controls and associated evidence without need to re-document explicit approval of services if the ports associated with their use are already approved. In addition, Duke seeks updated measures to provide examples of how services may be documented.	

Duke Energy requests the inclusion of the “(or logical ports)” flexibility in Part 1.3 to mirror Part 1.1 particularly since Management Modules are included and are known to have poor documentation on older models such that open port data may only be available from port scans.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

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	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 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	

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	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
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	
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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	

Comment	
Please see comments submitted by the Edison Electric Institute	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	

7. CIP-010 Requirement R1 currently requires Responsible Entities to develop a baseline configuration, authorize changes to the baseline, and document the changes. The SDT proposes to revise Requirement R1 to remove the reference to baseline configurations. The proposed revisions require the authorization of changes to Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible ports, security patches applied, and SCI configurations. Do you agree with the proposed changes? 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

Consider revising to clarify the lower threshold of what is included in the term *baseline.* Otherwise, this language may be interpreted to include administrative changes in nature and have no impact to the cybersecurity posture of the cyber asset.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

1. SRP interpret this to mean providing baselines will not be required for evidence. This does not state anything about physical, only virtual. Please clarify requirements for Physical, and backward compatability.

2. SRP recommends changing logical network accessible ports to logical network accessible services to be in alignment with the other proposed changes. SRP also believes SCI configurations is redundant. SCI configuration is included as part of the “Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible services and security patches applied of the virtualization and storage system.

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: Refer to our comments in the QUESTION 1 definitions. Considerations could be existing revised language to meet the intent of the SAR and a revision to CIP-010 R1.1.

A. The baseline documentation requirement represents the current configuration of a BCS/BCA with the objective of maintaining the security posture of the BCS/BCA, otherwise the changes have no basis.

The virtual image shouldn't be captured as a baseline because: 1) for an active virtual image, it should be a VCA that has its own baseline; 2) for a dormant virtual image, it is similar to a powered off physical cyber asset, as long as you maintain a base image for compliance all the time, it can be used when the dormant virtual image is turned on. In addition, the configuration baselines are not for the proposed definitions and applicability for SCI, SCA and management modules (See our comments for Question 1).

Recommendation: Restore CIP-010-3 language.

Likes 1	Lincoln Electric System, 1, Johnson Josh
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

Comments: Refer to our comments in the QUESTION 1 definitions. Considerations could be existing revised language to meet the intent of the SAR and a revision to CIP-010 R1.1.

The baseline documentation requirement represents the current configuration of a BCS/BCA with the objective of maintaining the security posture of the BCS/BCA, otherwise the changes have no basis.

The virtual image shouldn't be captured as a baseline because: 1) for an active virtual image, it should be a VCA that has its own baseline; 2) for a dormant virtual image, it is similar to a powered off physical cyber asset, as long as you maintain a base image for compliance all the time, it can be used when the dormant virtual image is turned on. In addition, the configuration baselines are not for the proposed definitions and applicability for SCI, SCA and management modules (See our comments for Question 1).

Recommendation: Restore CIP-010-3 language.

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 agrees with the proposed revisions that remove references to baseline configuration because they provide significant relief from baseline tracking and seem to better align with general change management practices. However, the deletion of the term “configuration” from “configuration change management” throughout the revisions may cause a great deal of confusion. Change management covers a wide breadth of “changes” from items considered “baseline configurations” to other non-material changes that do not affect a baseline. Differences in interpretation or definition of “change management” could lead to a dispute with Regional Entities and present a compliance risk. ISO-NE recommends that the SDT make further revisions to clarify which “changes” that require change authorization and testing.

ISO-NE also recommends that the SDT remove CIP-010 R1 Part 1.1.6 and create a new requirement to align the applicability for SCI.

Furthermore, ISO-NE recommends that the added language to CIP-010 R1.3, “...that minimizes difference with the production environment…” be deleted because CIP-010 Part 1.3.2 requires that the differences between the test environment and production environment be documented.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

In *CIP-003-3 we had requirement R6 that stated “Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.” CIP-010 R1 was developed to put an emphasis*

on configuration management . It now appears CIP-010-5 is reverting back to authorizing a change and not assuring that you have a trusted configuration.

Baseline management is critical for system integrity, being able to detect and correct unauthorized changes, and insure that machines are properly configured, patched, and up-to-date. Removing the requirement to maintain baseline configurations will leave significant security gaps, would lead to significant visibility issues into the configuration state of the Cyber Asset, ultimately leaving Responsible Entities blind to unknown vulnerabilities within the Cyber Assets. Baselining tools are becoming more and more capable of automating the process for baselining an Entities' environment – so there is no reason to strip this out of the standard. Even with the addition of virtualization, one would be able to baseline (and monitor baselines) for any virtual machines that the entity uses.

R1.4 will require entities to monitor for unauthorized changes. Unless they have a baseline to compare to, they will not be able to know when a change is made.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with this approach. This reduces administrative burden.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	

Response
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD
Answer	No
Document Name	
Comment
CHPD agrees with the changes, but as stated before, CHPD does not agree with the CPU and memory isolation requirements. The affinity rules should not be included in the list of configuration items that require authorization for change.
Likes 0	
Dislikes 0	
Response
Victoria Mordi - Entergy - 3,7,9 - SERC
Answer	No
Document Name	
Comment
While Entergy does agree with the approach being suggested, the switch from a port focus to a services focus adds an additional challenge. Network services are generally difficult to identify programmatically since many can be configured off default registered ports or use ports in theephemeral ranges that change with each use. The wording used here would seem to indicate that ports can only be used if the service cannot be identified, this would certainly lead to requiring a mixture of methodologies used for identification for each device. Entergy would recommend this wording be changed to identify that either the port or the service should be identified to give entities the flexibility to use either in order to maintain consistency in their program, which would reduce human performance errors. Additionally, more definition should be wrapped around what the Regulator means by service? Do they mean the network protocol or the service running on the asset that is network accessible. An example would be do they want https or Apache Web Service identified? This lack of definition would make it difficult to identify what monitoring would need to be put in place and what evidence would need to be gathered to meet this standard.
Likes 0	
Dislikes 0	
Response
Adrian Andreoiu - BC Hydro and Power Authority - 1
Answer	No

Document Name	
Comment	
It is not clear if the maintenance and upkeep of the current baseline and previous baselines is still required. BC Hydro SME team requests that the wording of the CIP-010 Requirement R1 be clarified to reflect if baselines are not needed any more. The technical rationale for CIP-010 R1 also needs more clarity if the previous baselines are required to be maintained as change records (time period until they should be kept as record and maintained) and what additional controls are proposed, if any, if the baseline is only one of the controls.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Please provide additional clarification and contextually relevant guidance to draw out the SDT's intent with the definition of "SCI." Moreover, the inclusion of baseline elements requires more context to the new term "SCI."	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No

Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AEPCO is signing on to ACES comments, please see below: The question does not include the new definition for Self-Contained Application, so ACES cannot answer “Yes.” . ACES suggests removing the definition and term “Self-Contained Application” .	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
It is unclear if the addition of “The production environment does not include devices being actively remediated and logically isolated.” indicates that assets currently listed in a remediation action plan do not need to be included in annual CVA.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No

Document Name	

Comment

SDT has created an uncalled for scenario where they have removed Baselines but left the baseline elements intact, which is causing significant confusion amongst SMEs.

Requiring CM as method of compliance will set a serious challenge and will limit ability to secure system as CMs do not include security baseline information, only the proposed changes, but assessments are never included in CM, just a summary of results.

This whole approach will result in inaccurate and subjective application and often result in contention with compliance and auditors.

Current CIP-010 standards and requirements are matured and industry has made significant progress developing good controls. There is absolutely no reason to change as these changes do not improve security but are detrimental.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

CIP-010 R1, request that the SCI requirement into a separate Part.

Remove the “OR” statements in Part 1.1. Applicable Systems. Placing the SCI requirement into a separate Part could resolve this

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE is concerned 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. 4), CM-2 Baseline Configuration, which states, “*Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture*.”

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 question does not include the new definition for Self-Contained Application, so ACES cannot answer “Yes”. ACES suggests removing the definition and term “Self-Contained Application”.

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports Marty Hostler and Northern California Power Agency comments.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions caused this no vote for this standard.

We agree with the removal of the administrative function of documenting a baseline.

Request c “minimal differences” be changed to “minimal differences, as determined by the entity”

Many of the Applicable Systems use only AND – some Applicable Systems use “OR” . For example, Part 1.1 says “SCI hosting High or Medium Impact BCS or their associated:” It is the "or their associated” that is in question. This probably means that the SCI is applicable but this is not clear.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

SPP offers the following comments and questions for the SDT consideration for Question 7:

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.

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.

Recommend the SDT define and provide an interpretation in the scope of what it means by “Authorized Changes”.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We agree with this approach. This reduces administrative burden.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

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 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	
Three comments on R1.3. These comments are repeated for CIP-010 R3.2. 1) request removal of “minimizes differences with the production environment” because new language is a) subjective, b) better suited to the measures and c) the previous language is sufficient 2) if this language cannot be removed, request clarification that the entity determines “minimal differences” 3) suggest that the intent is to a) test and b) document what was tested. CIP-010 R1, request that the SCI requirement into a separate Part. Same comment made for CIP-010 R1. Request clarification – there are several ways to read the nested ORs included in the Applicable Systems section for SCI. Many of the Applicable Systems use only AND – some Applicable Systems use OR. For example, Part 1.1 says “SCI hosting High or Medium Impact BCS or their associated:” Suggest reviewing the definition for better clarity.	
Likes 0	
Dislikes 0	
Response	

Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy recommends changing logical network accessible ports to logical network accessible services to be in alignment with the other proposed changes. SCI configuration is included as part of the “Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible services and security patches applied of the virtualization and storage system.	
Likes 0	
Dislikes 0	
Response	

Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
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	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Please see comments submitted by the ISO/RTO Council Standards Review Committee.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	
CIP-010, 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. The proposed change decreases clarity (in terms of what must be done to demonstrate compliance). **Recommendation:** Reinstate the concept of “*baseline configuration.*” CIP-010, R1 - Likewise, removing the word “configuration” from the term “configuration change management” (both in the title of CIP-010, Table R1 and throughout the text of R1), may cause a great deal of confusion since the more generic term, “change management,” can be interpreted to include a wider breadth of “changes” than those limited to “baseline configuration” and may substantially expand the scope of this requirement with other non-material changes. **Recommendation:** Reinstate the term “*configuration change management*” in the title of CIP-010, Table R1 and throughout the text of R1. Part 1.1.3 – Typically, Self-Contained Applications are considered custom software which is already covered under the existing standard and as such would not require a revision. **Recommendation:** Explain why this clarification is needed.	

Part 1.1.4 – SRC agrees that logical network accessible ports alone only tell part of the story and supports the SDT's proposal to include services. That said, the shift away from logical network accessible ports to services does not significantly change the security benefit achieved; however, it does make it more difficult for an entity to define and may imply that defined ports do not need to be included.

Recommendation: SRC recommends the SDT retain the concept of ports and define a new term, "ephemeral ports;" i.e. the listening ports that initiate the conversation, as a focal point for protection and security. This would allow the industry to move away from port ranges.

Part 1.1.6 – The first three bullets are very specific and well defined. The fourth bullet is very vague and draws in everything else that is not defined, making it very difficult for entities to comply with.

Recommendation: Clarify the types of services intended by the fourth bullet so there is consistency across the ERO.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the proposed modifications to revise Requirement R1 to remove the reference to baseline configurations.	
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 supports the SDT's direction here to provide a forward-looking, objective-based requirement and eliminate the documentation exercise of maintaining baseline inventories. However, for R1.1.2, Southern requests the SDT consider adding the concept of "installed" back as it is done in R1.1.3. Also, please consider re-ordering the proposed requirements in order to potentially split requirements for stand-alone systems and Self-Contained Applications. For example, R1.1.3 could focus on authorizing change to the SCAs when they are changed in a repository and not as they are automatically deployed from there to each 'applicable systems'. Additionally, we request the SDT provide further guidance on the components of "SCI configurations" for which changes must be authorized. The bulleted list in CIP-010 R1.1.6 provides some guidance but is not encompassing. Under CIP-010 R1.1.6, Southern requests that the SDT consider removing the first bulleted item "Enforces electronic access controls that…" as that is essentially the same as the second bulleted item "Enforces logical isolation between…"	

Under CIP-010 R1, Southern requests the SDT consider addressing the scenario, and provide alternative requirement language, as to “when” authorization has to occur. For example – are changes to a virtual desktop image residing in a BCSI repository required to be authorized at the time the image is updated, or when the updated image is deployed into a production environment? Or both?

Under CIP-010 R1.2, Southern requests the SDT consider removing Part 1.2.1 based on its lack of practicality. In recent audits of this requirement Part, auditors have expressed the expectation that Part 1.2.2. should include a check of all security controls to ensure they were not adversely impacted, thereby making the performance of Part 1.2.1. moot. Additionally, Southern recognizes that with many types of changes, it is not possible to predict all possible security controls changes that may take place with a change, and therefore most entities have adopted best practices to thoroughly check security controls following the change, making Part 1.2.1 useless from a security standpoint.

Additionally, Southern is concerned that the language in CIP-010 R2.1 would still force entities to maintain “documentation” the same as or similar to a “baseline configuration” in order to comply with R2. Southern requests the SDT consider this dilema and possibly propose alternative language for R2 that would align it with the proposed changes to R1. For example – in R2, the phrase “items described in R1, Part 1.1” are essentially the components of the former “baseline”; in order to monitor those items every 35 days for changes to those items, you must first have documentation, lists, or scan results of those items so that you can compare and detect any unauthorized changes to them. Likewise, the requirement does not dictate that an entity must monitor authorized changes, but only “unauthorized” changes. Therefore, for an entity at audit that has had no “unauthorized” changes, the activity can become a deep-dive “prove-the-negative”.

To align the direction of R1 towards “change management”, Southern requests the SDT consider removing the word “configuration” in the Measures of R2.1 and replace it with something akin to:

R2.1: An example of evidence may include, but is not limited to, documentation or logs showing that monitoring for changes to the items in Part 1.1 is conducted, along with records of investigation for any unauthorized changes that were detected.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

We agree with this approach. This reduces administrative burden.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

No comments	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes that the verbiage should be updated to reflect logical network accessible **services** as opposed to ports.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change and agrees with comments provided by EEI for this survey question	
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	

There is no timeline for authorizing changes, but we like the option to define that timeline ourselves. There should be a provision for urgent changes – like zero day vulnerabilities, that would allow authorization after a change has occurred.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments for the SDT's review and consideration:

1. Consider whether the purpose statement should be revised to address the broader scope of the proposed revisions.

2. In the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

3. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

4. In requirement R1.1.6, the following revision is recommended for clarity:

1.1.6. Enforces electronic access control that permits only controlled communications that are [needed/necessary] between systems with different impact ratings hosted on SCI.

5. In the proposed revisions for requirement R1.3.1, the proposed verbiage is unclear. The following revision is recommended for clarity:

1.3.1. Prior to implementing any authorized change in the production environment, except during a CIP Exceptional Circumstance, test the authorized changes in a test environment that has minimal, documented/authorized differences when compared with the production environment…

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change and agrees with comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Suggest reviewing the definition for better clarity.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	

Answer	Yes
Document Name	
Comment	
This change seems somewhat negligible. Auditors will still likely expect similar documentation as they always have to ensure that all changes are captured and approved and that there is a complete population to audit. The theory and objective of the changes seem sound but the actual benefit of these changes seem as if they will be minimal.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes

Document Name	
Comment	
AEP supports changes regarding baseline configurations. While baselines will remain a critical record for entities to maintain, they should not be used for compliance purposes. Instead, we agree with the modifications that place the emphasis on monitoring unauthorized changes (to the items described in Requirement R1, Part 1.1). The process of tracking and maintaining records for all changes to a baseline represent an unnecessary compliance burden that offers few protections yet places burdensome recordkeeping on entities for no material reliability benefit.	
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	
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	
There is no timeframe clarified in CIP-010 R1 for the authorization to occur. Suggest clarifying as: “Prior to the change, authorize changes to:” as the lead in statement. We further suggest that if this change is made that the CEC Exception also be included to allow for emergency change to be performed ahead of formal documented authorization.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
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	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change and agrees with comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes

Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-010, R1, PG&E supports the modfications and the input provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 7.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the changes regarding baseline configurations. While baselines will remain a critical record for entities to maintain, they should not be used for compliance purposes. Instead, we agree with the modifications that place the emphasis on monitoring unauthorized changes (to the items described in Requirement R1, Part 1.1). The process of tracking and maintaining records for all changes to a baseline represent an unnecessary compliance burden, that offers few protections yet places burdensome recordkeeping on entities for no material reliability benefit.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	

Answer	Yes
Document Name	
Comment	
While we appreciate the revisons to CIP-010 R1, is the expectation that we would just need to provide a set of tickets where we said the baseline changed, but not have to back it up with baseline documentation? Would the change ticket now need to be in more detail to clearly indicate what element(s) of CIP-010 R1.1 changed so we don't have to provide baseline documentation? For example, “updated Windows machines with patches for released in {MONTH] {YEAR}” or “updated machine X with SFTP service”? PNMR expresses support of comments by John Galloway, On Behalf of: Michael Puscas, ISO New England, Inc.	
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	

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

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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
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	

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
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	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
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 Cantwell - Lower Colorado River Authority - 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	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

8. The SDT modified CIP-010 Requirement R3 Part 3.3 to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. The revised requirement allows the use of remediation VLANs to perform active vulnerability assessments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

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

The SRC greatly appreciates the following changes and clarifications proposed by the SDT:

- Part 3.2: addition of "*per system capability*"
- Part 3.3: use of "*previously assessed configurations*" allows for the use of gold images

Recommendations:

- Replace the last sentence of Part 3.3; i.e. "*The production environment does not include devices being actively remediated and logically isolated*," with the following: "*Remediation or mitigation action items must be completed prior to production use*." This meshes with Part 3.4 and clarifies that all vulnerabilities must be remediated prior to production use as opposed to remediated prior to placing in an ESP environment.
- Clarify that annual active vulnerability assessments would not require the use of remediation VLANS

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	

Comment

Request explanation. This language is about "connecting." Elsewhere language is about "isolating." Please explain this switch.

Request clarification - what is the change when discussing physical connection or active communication?

Request clarification of the requirement because the OR is confusing. Would it be easier to understand with two sentences instead of one long sentence?

Request clarification of the first and last sentences in this requirement. What is the difference between "logically isolated" and "not logically connected?" Please clarify how to read the first sentence's ORs.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The use of an undefined term, “logically connecting” has the potential to create confusion when included within a NERC CIP Reliability Standard Requirement. The Standard Processes Manual provides direction for when a NERC Glossary of Terms definition is needed, notably that certain criteria should determine whether a new or revised definition is needed (see Appendix 3A (ROP) Standard Processes Manual, Section 5.1). The primary factor for determining whether a NERC defined term is needed rests on whether the term can be understood using a standard collegiate dictionary. For many IT terms commonly in use, the standard collegiate dictionary is rarely helpful. For example, the term logically connected is not defined by Merriam-Webster. The NIST Information Technology Laboratory (Computer Security Resource Center On-line Glossary of Terms (https://csrc.nist.gov/glossary) includes “logically connecting” and similar terms such as “logically connected, logical connection, etc.” Unfortunately, a definition that aligns with the term “logically connecting” that might provide insights necessary to ensure that those responsible for compliance have a common understanding of what is being proposed in Requirement R3, Part 3.3. is unavailable. EEI recommends the term be defined or direction be provided within the Technical Rationale to ensure a consistent understanding. EEI requests for clarification whether cyber vulnerability assessments must be performed in the VLAN environment and then switched to production.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	No
Document Name	
Comment	

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 8

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 explanation. This language is about “connecting.” Elsewhere language is about “isolating.” Please explain this switch.

Request clarification - what is the change when discussing physical connection or active communication?

Request clarification of the requirement because the OR is confusing. Would it be easier to understand with two sentences instead of one long sentence?

Request clarification of the first and last sentences in this requirement. What is the difference between “logically isolated” and “not logically connected?” Please clarify how to read the first sentence’s ORs.

Suggest reviewing the definition for better clarity.

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 SRC.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We support the concept; however, we need more information on the use of remediation VLANs and the evidence required. Please consider a webinar and/or additional details in the technical rationale. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-010, R3, Part 3.3. PG&E does have concerns and supports the input provided by EEI.	
Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP Votes **YES** to this one with no comments. This is an edited response and the button option to change the vote is grayed out. Thank you.	
Likes 0	
Dislikes 0	
Response	

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard	
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	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
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	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Request explanation. This language is about “connecting.” Elsewhere language is about “isolating.” Please explain this switch. Request clarification - what is the change when discussing physical connection or active communication? Request clarification of the requirement because the OR is confusing. Would it be easier to understand with two sentences instead of one long sentence? Request clarification of the first and last sentences in this requirement. What is the difference between “logically isolated” and “not logically connected?” Please clarify how to read the first sentence’s ORs.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
Too much compartmentalization based on non-industry standard definition. Please review NIST Publication 800-125 (virtualization guidelines) and apply controls, based on Terms such as Management Systems, Guest, Hosts, Network virtualization, Infrastructure virtualization (Mixed Trust, Resources sharing, high-watermarking) and similar guidance that is used by Industry, SME and vendors. SDT approach is complicated and confusing which will result in different interpretation by SMEs and ERO.	
Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI's 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	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
The use of an undefined term, “logically connecting”, has the potential to create confusion when included within a NERC CIP Reliability Standard Requirement. Additional clarification is needed on whether cyber vulnerability assessments are required to be performed in the VLAN environment and then switched to production, or could a VCA or SCI be built in its production environment but not activated until the cyber vulnerability assessment is performed and is determined to be ready for activation in the production environment.	
Likes 0	

Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS agrees with the need for a definition of “logically connecting”. This would allow the removal of human error traps associated with a vague interpretation of the definition down the road.	
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 since it is not clear how an entity is to perform a true vulnerability assessment on a Cyber Asset unless it is connected to the target network. Connecting a Cyber Asset to a network other than the target network will net differing results and require the reconfiguration of the Cyber Asset from the remediation network to the target network.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE 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 changes since it is not clear how an entity is to perform a true vulnerability assessment on a Cyber Asset unless it is connected to the target network. Connecting a Cyber Asset to a network other than the target network will net differing results and require the reconfiguration of the Cyber Asset from the remediation network to the target network.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
As stated earlier, logical isolation is not a defined term. We would like to see an actual definition for "logical isolation"	
Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	

Comment
Oklahoma Gas and Electric supports the comments provided by EEI.

Likes 0	
Dislikes 0	

Response

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

Comment
R3.3 ‘The production environment does not include devices being actively remediated and logically isolated.’ The language of this requirement lacks clarity around undefined terms: ‘logically connecting’, ’additional’, ‘devices’, ‘remediated’, and ‘logically isolated’, resulting in unenforceability. The requirement does not include consideration of CPU/memory sharing as seen with other logically isolated systems. The language also seems to be somewhat circular in that the ‘production environment’ includes an exclusion after the requirement language. Suggested Comment: R2.1 lacks inclusion of SCI and Management Systems for High Impact BCS and associated EACMS, PCAs. This does not align with their inclusion in most of the other requirements within the standard and reduces the protections required under the current standard language. The technical rationale does not address why it is not needed for SCI.

Likes 0	
Dislikes 0	

Response

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

Comment

We support the concept; however, we need more information on the use of remediation VLANs and the evidence required. Please consider a webinar and/or additional details in the technical rationale.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

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

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

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

Answer	No
Document Name	

Comment

It is unclear to us whether a scan will be needed for all installations and that the previous concept of a group of baselines is no longer acceptable. This amount of additional work is excessive and does not alleviate any additional cybersecurity risk. We request that the SDT make it very clear using a scan from a previously installed Cyber Asset, VCA or SCI that is similarly configured is acceptable to demonstrate compliance with R3.3.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Remediation VLANs are not defined and may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.	
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	
CIP-010 Requirement R3 Part 3.3 uses the undefined term "previously assessed configuration" which could be interpreted as a byte-for-byte copy of a golden image, or could be referring to the items defined in Part 1.1. ISO-NE has concerns that the industry will gravitate to the most conservative interpretation of the term. ISO-NE recommends that the SDT include Part 1.1 items in Part 3.3 to further clarify this requirement. ISO-NE recommends that the SDT clarify the level of logical isolation that is expected to keep the device out of the production environment when using a remediation VLAN.	
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	
Answer	No
Document Name	
Comment	
Logically connected should be further defined to reduce the likelihood of misinterpretation.	
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
Comments: The revisions to CIP-010-3 R3.3 are not clear (See our comments for QUESTION 1). We have not observed challenges with remediation VLANs in the existing CIP requirements. This is because remediation VLANs can be managed within the ESP as a hot standby VLAN when connected to a layer 2 (data link) BCA switch or connected to a non-CIP switch. The language “The production environment does not include devices being actively remediated and logically isolated” does not resolve security concerns; i.e., depending on what type of logical isolation is acceptable? Additionally, this term is subjective. If logical isolation is allowable for a non-ESP model, it could also be allowable for an ESP model meaning as long as a Remediation VLAN is logically isolated from the BCS VLAN on the same switch, it doesn’t need to be within the 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
Comments: The revisions to CIP-010-3 R3.3 are not clear (See our comments for QUESTION 1). We have not observed challenges with remediation VLANs in the existing CIP requirements. This is because remediation VLANs can be managed within the ESP as a hot standby VLAN when connected to a layer 2 (data link) BCA switch or connected to a non-CIP switch. The language “The production environment does not include devices being actively remediated and logically isolated” does not resolve security concerns; i.e., depending on what type of logical isolation is acceptable? Additionally, this term is subjective. If logical isolation is allowable for a non-ESP model, it could also be allowable for an ESP model meaning as long as a Remediation VLAN is logically isolated from the BCS VLAN on the same switch, it doesn’t need to be within the ESP.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	

Comment
These changes allow for more flexibility regarding VAs in virtual space. However, consider revising language to be more outcome-based, e.g., reducing the risk to BCS's inherent introduction of new cyber assets and/or technologies.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE seeks clarification as to whether the SDT is using the phrase “logically isolated” in the same context as proposed CIP-005-7.	
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	
In CIP-010 R3 Part 3.3, the use of “device” doesn’t appropriately cover virtual machines or Virtual Cyber Assets. Therefore, Tacoma Power recommends the following change: “The production environment does not include systems or components being actively remediated and logically isolated.”	
Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Suggest reviewing the definition for better clarity.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
CHPD supports the efforts of the SDT here to make deployment and remediation of devices easier.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	

Comment

GSOC provides the following comments for the SDT's review and consideration:

1. Generally, the formatting of applicable systems within the applicable systems column should be evaluated for consistency of format.

2. In the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

3. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

4. In the proposed revisions for requirement R3.2.1, the proposed verbiage is unclear. The following revision is recommended for clarity:

3.2.1. Perform an active vulnerability assessment in a test environment that has minimal, documented/authorized differences when compared with the production environment…

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
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

Would like to see the standard require a credentialed vulnerability assessment vs an active vulnerability assessment per asset capability and/or allow for passive analysis which is less intrusive and often more effective than active scans.

Likes 0	
Dislikes 0	

Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
We support the concept; however, we need more information on the use of remediation VLANs and the evidence required. Please consider a webinar and/or additional details in the technical rationale.	
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 supports the SDTs direction for CIP-010 R3 Part 3.3 to allow remediation VLANs to perform active vulnerability assessments.	
Likes 0	
Dislikes 0	

Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
We agree with the introduction of remediation VLANs, however, for the sake of backwards compatibility, wording should be added for physical vulnerability assessment tools that would reside on a physical test network for non-virtualized or hybrid environments.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the proposed modifications to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. Duke Energy recommends adding clarity on what constitutes “logically connecting”. Duke Energy noticed that the approach and requirement language here seem inconsistent with the language in proposed CIP-005 requirements. It is not clear if it is intent that only the network interface for a VCA must be logically isolated into the remediation VLAN, or if the CPU/memory-sharing isolation requirements apply as well. Conceptually the intent makes sense, but the standard should be clear about what level of logical isolation is expected to keep the device out of the production environment when using a remediation VLAN.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
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	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	
Laura Nelson - IDACORP - Idaho Power Company - 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	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
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	
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	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
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	

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	

Please see comments submitted by the Edison Electric Institute	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	

9. CIP-002-5.1a includes exemption 4.2.3.2, which exempted Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. In the development of conforming changes, the SDT determined that the exemption should be split into two distinct exemptions to adequately cover all cyber systems associated with conforming changes. The SDT established those conforming changes in proposed Exemptions 4.2.3.2 & 4.2.3.3. Do the changes clearly identify the exempted cyber systems? 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

Proposed language lacks the clarity to provide a consistent application.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

1. As SRP reads the definition of what is in scope is not clear from what is stated in the exemption. Clarity is needed due to the vagueness with more details or more of an explanation.

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: Due to the use of the ‘logical isolation’ term, and SCI term the changes to 4.2.3.2 & 4.2.3.3 are not needed.

A. Based on our comments in QUESTION 1 and Question 2, the logical isolation for non-routable connections between CIP Cyber Assets is not required by the SAR. The current exemption for communications equipment and links between ESPs implies multiple physical locations.

B. If the SDT intended to address the exclusions of discrete communications links between ESPs, then we suggest a revision to CIP-006-6 R1.10. If NERC is interested in addressing confidentiality and integrity between multiple ESPs (i.e., a super ESP), then we suggest a new SAR to add additional requirements.

Recommend:

- modifying 4.2.3.2 and removing 4.2.3.3.
- Change 4.2.3.2 to clarify the discrete ESPs to span one or more geographic locations such as:

"Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters, and where an individual ESP spans one or more geographic locations."

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

Exemption 4.2.3.3 needs to be revised to provide further clarity. This appears to be an exclusion for "cyber systems" associated with communication links between discrete ESPs. The new language doesn't provide the clarity of the approved exemption.

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

Comments: Due to the use of the 'logical isolation' term, and SCI term the changes to 4.2.3.2 & 4.2.3.3 are not needed.

Based on our comments in QUESTION 1 and Question 2, the logical isolation for non-routable connections between CIP Cyber Assets is not required by the SAR. The current exemption for communications equipment and links between ESPs implies multiple physical locations.

If the SDT intended to address the exclusions of discrete communications links between ESPs, then we suggest a revision to CIP-006-6 R1.10. If NERC is interested in addressing confidentiality and integrity between multiple ESPs (i.e., a super ESP), then we suggest a new SAR to add additional requirements.

Recommend:

- modifying 4.2.3.2 and removing 4.2.3.3.
- Change 4.2.3.2 to clarify the discrete ESPs to span one or more geographic locations such as:

"Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters, and where an individual ESP spans one or more geographic locations."

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 replacement of Cyber Assets (a defined term) with cyber systems (an undefined term) introduces ambiguity and requires a Registered Entity to self-define cyber systems. This can lead to misinterpretations and disputes between Regional Entities and Registered Entities.

ISO-NE recommends either defining "cyber systems" or reverting back to the defined term Cyber Assets.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
CIP-002-7, 4.2.3.2. states: “Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).” To ensure that this is properly understood *a definition of “logical isolation” is required.*	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
We appreciate the effort to be consistent with the other exemptions. We do not agree that the exemptions for 4.2.3.1, 4.2.3.2 and 4.2.3.3 clearly identify the exempted cyber systems. We believe term “cyber systems” indicates a broader scope than is intended. This could lead to developing each “cyber system” construct that could lead to under or over scoping BES Cyber System assets for CIP-002. We believe that “systems” as used in the other exemptions relates to things that are categorized beyond “cyber systems”. We do recognize “systems” could include cyber systems at these related assets. Example for 4.2.3.2 & 4.2.3.3: An entity could scope a cyber system as a communication system where the system would reasonably include substation RTUs, channel banks, digital cross connects, microwave radios, etc. Although in our current version, many entities have included RTUs as BES Cyber Assets, the proposed change would lend to 1) removing RTUs from our CIP Programs or 2) expanding the net to Cyber Assets that have been considered part of the current exception because they are now included as part of the communication system. We realize there are ways around this example, but we wanted to highlight this for the purposes of our discussion. For exemption 4.2.3.1 consider removing “cyber” as shown in the following edit: **4.2.3.1.** Systems at Facilities regulated by the Canadian Nuclear Safety Commission.	

For exemptions 4.2.3.2 & 4.2.3.3, we suggest keeping the exception scope to assets that are defined NERC Glossary terms as shown below:

4.2.3.2. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Also, please provide clarification why the edits included reducing from “communication networks and data communication links” to just “communication links.”

Note: These comments apply to all of the standards in this ballot.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Suggest clarification on the geographic locations.

Request clarification – is the cyber system equivalent to Cyber Asset? We note that Cyber Asset is a defined term. Cyber system is not a defined term.

Request clarification that 4.2.3.2's updates are equivalent to the previous language. Are the demarcation points the same? Explicit exclusions set better expectations

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We appreciate the effort to be consistent with the other exemptions. We do not agree that the exemptions for 4.2.3.1, 4.2.3.2 and 4.2.3.3 clearly identify the exempted cyber systems. We believe term "cyber systems" indicates a broader scope than is intended. This could lead to developing each "cyber system" construct that could lead to under or over scoping BES Cyber System assets for CIP-002. We believe that "systems" as used in the other exemptions relates to things that are categorized beyond "cyber systems". We do recognize "systems" could include cyber systems at these related assets.

Example for 4.2.3.2 & 4.2.3.3: An entity could scope a cyber system as a communication system, where the system would reasonably include substation RTUs, channel banks, digital cross connects, microwave radios, etc. Although in our current version, many entities have included RTUs as BES Cyber Assets, the proposed change would lend to 1) removing RTUs from our CIP Programs or 2) expanding the net to Cyber Assets that have been considered part of the current exception because they are now included as part of the communication system. We realize there are ways around this example, but we wanted to highlight this for the purposes of our discussion.

The exemption language in section 4.2 of every CIP standard will need to be addressed.

For exemption 4.2.3.1 consider removing "cyber" as shown in the following edit:

4.2.3.1. Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

For exemptions 4.2.3.2 & 4.2.3.3, we suggest keeping the exception scope to assets that are defined NERC Glossary terms as shown below:

4.2.3.2. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Also, please provide clarification why the edits included reducing from “communication networks and data communication links” to just “communication links’”

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure

Likes 0	

Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for 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 changes since they do not clearly identify the exempted cyber systems. The new version uses the undefined term cyber systems as opposed to the original using the defined Cyber Assets term. CEHE agrees that revisions are needed since the original resulted in equipment used by carriers to be exempted while the same equipment used by a Registered Entity on a private communications network was considered in scope. The following changes have been proposed. 4.2.3.2. Cyber assets whose function is only to provide connection to external communication networks, as defined by demarcations set by the Registered Entity, that are logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).	

4.2.3.3. Cyber assets whose function is only to provide connection to external communication networks, as defined by demarcations set by the Registered Entity, between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
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 since they do not clearly identify the exempted cyber systems. The new version uses the undefined term cyber systems as opposed to the original using the defined Cyber Assets term. SIGE agrees that revisions are needed since the original resulted in equipment used by carriers to be exempted while the same equipment used by a Registered Entity on a private communications network was considered in scope. The following changes have been proposed. 4.2.3.2. Cyber assets whose function is only to provide connection to external communication networks, as defined by demarcations set by the Registered Entity, that are logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI). 4.2.3.3. Cyber assets whose function is only to provide connection to external communication networks, as defined by demarcations set by the Registered Entity, between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	

Answer	No
Document Name	

Comment

It is still unclear what the phrase “logical isolation” will mean as it gets implemented in many different scenarios provided in this draft of the standards even though it has been used as an accepted term in the explanations provided with these drafts. Exemption 4.2.3.3. also uses this phrase as if it will be universally clear what devices will be used in the implementation of logical isolation. Logical isolation is not a defined term, and though it is attempting to be used as a replacement for ESP, plus more, there are many changes to the standards that are not places where ESP was used or required, and now logical isolation is being used as a universally accepted term without examples or further discussions. The exemptions as listed do not make it clear where that line of demarcation will be nor have examples been provided in meaningful ways. Similar to when CIP-003 was released, there were many diagrams and explanations provided to help entities walk through the different scenarious that could be used in implementation and to convey the intent of the standard.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

AZPS does not believe these changes clearly identify the exempted cyber systems. We believe that the undefined term “logical isolation” causes an unclear interpretation. We also feel that the exclusion of the “communication networks” could expand the scope of what’s needed to remain compliant.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

Changes made to CIP-002 exemptions noted in 4.2.3.2 and 4.2.3.3 do not provide a clear understanding of what is exempted because both use terms that are undefined. For 4.2.3.2, the defined term “Cyber Asset” has been replaced by an undefined term “cyber system”. Additionally, the currently approved CIP-002-5.1a exempts communication networks and communication links between discrete ESPs, while the proposed new CIP-002-7 Reliability Standard only exempts the communication links thus implying that the communication networks may now be subject to CIP Requirements.

In order to clearly define exempted Cyber Assets associated with communication networks, it is necessary for the Registered Entity to clearly designate the communication network components since communication network, communication systems or communication assets have no NERC definition. The following changes have been proposed;

- 4.2.3.2. Cyber Assets associated with communication networks, as defined by demarcations set by the Registered Entity, logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).
- 4.2.3.3. Cyber Assets associated with communication networks, as defined by demarcations set by the Registered Entity, between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Lastly, the undefined term “logical isolation” is used in both exemptions. As stated in our comments for Question 1, this term should be defined to ensure a clear and common understanding of both the Requirements and Exemptions are contained within the body of CIP Reliability Standards.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

AEPCO is signing on to ACES comments, please see below:

ACES does not agree with the new language. The definition of a Cyber Asset is very clear and well known by the industry. The new language “cyber systems” is not defined and could be interpreted differently by entities and auditors. An Entity can point to specific Cyber Assets easily. We also feel this change was not a part of the FERC order or in the scope of the SAR.

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

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

Answer	No
Document Name	

Comment

The language in *4.2.3.3* is problematic. It is unclear assets are performing the logical isolation in the Requirement. Cyber systems or the Cyber Assets, Virtual Cyber Assets, or SCI? While Dominion Energy is of the opinion, based on the language in the Requirement, that the latter assets (Cyber Assets, Virtual Cyber Assets, or SCI) are performing the activity, the current language could be interpreted as indicating the Cyber systems are performing the activity.

Suggested language is as follows:

Cyber systems associated with communication links between assets (Cyber Assets, Virtual Cyber Assets, or SCI) that perform logical isolation that extends to one or more geographic locations.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment
Many entities have virtualized systems and were compliant with CIP in recent audits. Please do not over complicate. Focus on security or where gaps exists. Only changes to BCS to include virtual environment and logical asset configuration is required.

Likes 0	
Dislikes 0	

Response

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

Comment
Request clarification – is the cyber system equivalent to Cyber Asset? We note that Cyber Asset is a defined term. Cyber system is not a defined term Request clarification that 4.2.3.2's updates are equivalent to the previous language. Are the demarcation points the same? Explicit exclusions set better expectations.

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

Likes 0	
Dislikes 0	

Response

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

Comment
Texas RE recommends defining the term “cyber system.” While it is noted in the technical rationale, the phrase “cyber systems” is not defined in NERC Glossary of Terms. Texas RE recommends defining the term “cyber systems” in the NERC Glossary or, alternatively, use the description provided in the technical rationale to reduce ambiguity in the requirement language. It is unclear whether that undefined term is associated with “system” in CIP CIP-006-7, CIP-007-7, CIP-009-7, CIP-010-5, the “Applicable Systems” column in all CIP standards parts. Texas RE inquires as to whether these changes would exclude Cyber Assets such as serial/IP converters, data diodes, protocol converters, etc. For example, a serial/IP converter may connect to a BCA serially but convert the protocol from serial to TCP/IP and is connected to a network Cyber Asset that operates at Layer 3 or higher of the OSI model. Texas RE would recommend providing examples to reduce ambiguity. Lastly, Texas RE seeks clarification on the phrase “one or more geographic locations.” Registered Entities have a variety of architectural layouts, which could result in confusion regarding the meaning of “one or more geographic locations.” For instance, entities may have two adjacent buildings that could be interpreted as either a single location or separate geographic locations.

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 new language. The definition of a Cyber Asset is very clear and well known by the industry. The new language “cyber systems” is not defined and could be interpreted differently by entities and auditors. An Entity can point to specific Cyber Assets easily. We also feel this change was not a part of the FERC order or in the scope of the SAR.

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	

Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
The change from Cyber Assets to cyber systems could expand this to devices that do not meet the “programable electronic device” portion of the Cyber Asset definition or be interpreted to include a limit on the scope. Cyber systems must be clearly defined.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for the CIP-002-5.1a exemption. PG&E does have concerns and supports the input provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	

Comment
We appreciate the effort to be consistent with the other exemptions. We do not agree that the exemptions for 4.2.3.1, 4.2.3.2 and 4.2.3.3 clearly identify the exempted cyber systems. We believe term “cyber systems” indicates a broader scope than is intended. This could lead to developing each “cyber system” construct that could lead to under or over scoping BES Cyber System assets for CIP-002. We believe that “systems” as used in the other exemptions relates to things that are categorized beyond “cyber systems”. We do recognize “systems” could include cyber systems at these related assets. Example for 4.2.3.2 & 4.2.3.3: An entity could scope a cyber system as a communication system, where the system would reasonably include substation RTUs, channel banks, digital cross connects, microwave radios, etc. Although in our current version, many entities have included RTUs as BES Cyber Assets, the proposed change would lend to 1) removing RTUs from our CIP Programs or 2) expanding the net to Cyber Assets that have been considered part of the current exception because they are now included as part of the communication system. We realize there are ways around this example, but we wanted to highlight this for the purposes of our discussion. The exemption language in section 4.2 of every CIP standard will need to be addressed. For exemption 4.2.3.1 consider removing “cyber” as shown in the following edit: **4.2.3.1.** Systems at Facilities regulated by the Canadian Nuclear Safety Commission. For exemptions 4.2.3.2 & 4.2.3.3, we suggest keeping the exception scope to assets that are defined NERC Glossary terms as shown below: **4.2.3.2. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure** associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI). **4.2.3.3. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure** associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations. Also, please provide clarification why the edits included reducing from “communication networks and data communication links” to just “communication links"

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 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

Request clarification – is the cyber system equivalent to Cyber Asset? We note that Cyber Asset is a defined term. Cyber system is not a defined term.

Request clarification that 4.2.3.2's updates are equivalent to the previous language. Are the demarcation points the same? Explicit exclusions set better expectations.

Suggest clarification on the geographic locations.

Request clarification – is the cyber system equivalent to Cyber Asset? We note that Cyber Asset is a defined term. Cyber system is not a defined term.

Request clarification that 4.2.3.2's updates are equivalent to the previous language. Are the demarcation points the same? Explicit exclusions set better expectations.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb 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; - Douglas Webb

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 9.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Neither 4.2.3.2 nor 4.2.3.3 provide a clear understanding of what is exempted because both use terms that are undefined. For 4.2.3.2, the defined term “Cyber Asset” has been replaced by an undefined term “cyber system”. Additionally, the currently approved CIP-002-5.1a exempts communication networks and communication links between discrete ESPs, while the proposed new CIP-002-7 Reliability Standard only exempts the communication links implying that the communications networks may now be subject to CIP Requirements. EEI recommends the restoration of the deleted language to ensure communications networks are exempt from the NERC Standards. Exemption 4.2.3.3 similarly identifies communication links but does not exempt communications networks. This should be corrected. Lastly, the undefined term “logical isolation” is used in both exemptions. As stated in our comments for Question 1, this term should be defined to ensure a clear and common understanding of both the Requirements and Exemptions are contained within the body of CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	

Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy suggests providing clatify to proposed language to provide consistent application.	
Likes 0	
Dislikes 0	
Response	

Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
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 considers the proposed language of 4.2.3.2 confusing, as it seems to suggest that under certain conditions communications links could provide logical isolation, which is surely not the SDT's intent. N&ST recommends simplifying as follows: "Cyber systems associated with communication links logically isolated from BCS or Shared Cyber Infrastructure (SCI)."	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The current standard uses "Cyber Asset," which is a defined term. Using "Cyber system" may lead to confusion and inconsistent applicability by using undefined terms. Also, "logical isolation" requires more definition to avoid issues with inconsistency.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	
Two new undefined terms stand out as key concerns in the proposed modifications to the exemptions in CIP-002 (4.2.3.2 and 4.2.3.3): Cyber systems and the concept of logical isolation. "Cyber system" is not defined in the **Glossary of Terms Used in NERC Reliability Standards** (BES Cyber System, yes, but not Cyber system). Nor is there a definition for "logical isolation." Each entity would be required to define these terms. This leaves	

some of the identification of exempted cyber systems (sic) up to the responsible entity and may introduce some areas of dispute between compliance monitoring and entity implementation activity.

Recommendation: Clarify the term “Cyber systems” and the concept of “logical isolation” so there is a level of consistency across the ERO.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC

Answer	No
Document Name	

Comment

Changes made to CIP-002 exemptions noted in 4.2.3.2 and 4.2.3.3 do not provide a clear understanding of what is exempted because both use terms (i.e. cyber systems and logical isolation) which are undefined. Undefined terms need to be defined to ensure a clear and common understanding..

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees to the proposed modifications to split the exemptions into two distinct exemptions to adequately cover all cyber systems associated with conforming changes.

Proposed 4.2.3.2 adequately addresses devices outside the identified logical isolation. Proposed 4.2.3.3 may exclude devices providing logical isolation that would otherwise be identified as EACMS. A lack of clarity with respect to the intended scope of this exclusion may result in auditor/entity interperetation disagreements. Assuming the intent is to exclude the connection between the devices, and not the e.g. VPN concentrators themselves, we propose modifying the language to something like “Cyber systems associated with communication links between “logical isolation” provided by Cyber Assets, Virtual Cyber Assets, or SCI where that isolation extends to one or more geographic locations.”

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

Below is a replication of our response to Question 1, which also addresses this question.

Cyber System (Undefined Term) – Modifications have been made under the exemptions section in CIP-002-7 which move from a Cyber Asset focus to a “cyber system” focus without a corresponding definition of what that term encompasses. With the difficulty of understanding the scope of this undefined term in virtualized environments, Southern recommends developing a definition for “cyber system”, such as:

1. **Cyber System:** *one or more Cyber Assets, VCAs, or SCI used to perform or achieve a cyber-based objective by a Responsible Entity or other party.*

2. Additionally, Southern requests the SDT to consider that Exemption 4.2.3.3. should be a sub-set of Exemption 4.2.3.2. rather than a stand alone item. It appears the main difference between the two exemptions is the distance between the points performing the logical isolation.

• Neither exemptions 4.2.3.2 nor 4.2.3.3 provide a clear understanding of what is exempted, possibly due to the change from “Cyber Asset” to the undefined “Cyber system”. Please see our comments above for a proposed definition of “Cyber System”. Also, the undefined term “logical isolation” is used in both exemptions. As stated in our previous comments, this term should be defined to ensure a clear and common understanding of both the Requirements and Exemptions.

• In order to clearly define exempted cyber systems associated with communication networks, it is necessary for the Registered Entity to clearly designate the communication network components since communication networks, communication systems, or communication assets have no NERC definition. Southern agrees with EEI comments addressing the following recommendations, but clarifying that the second exemption should be a sub-bullet to 4.2.3.2.:

• 4.2.3.2. Cyber systems associated with communication networks, as defined by demarcations set by the Registered Entity, logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

• 4.2.3.2.1 Cyber systems associated with communication networks, as defined by demarcations set by the Registered Entity, between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

BPA feels that the phrase “associated with” a BCS is less than desirable. The concept of “providing connectivity to” or “in the communications chain of but not providing the security controls to” a BCS describes the relationship more clearly.

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	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC supports the splitting of the exemptions to ensure appropriate coverage. However, it respectfully notes that additional clarity could be attained with small tweaks to the proposed exemption language: 4.2.3.2. Cyber systems associated with communication links that meet the following criteria: (1) are logically isolated from BES Cyber Systems or SCI; (2) do not provide logical isolation for BCS or SCI. 4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation beyond one geographic location.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
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	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
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	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
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	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 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	

James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 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	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

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

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	

Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

10. BCS and SCI are mutually exclusive by definition, however SCI poses a significant reliability risk to the Bulk Electric System. The SDT considered the risks associated with SCI and revised CIP-002 Requirement R1 to include the identification of SCI in Parts 1.3, 1.4, and 1.5. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC

Answer	No
Document Name	

Comment

Capital Power would like clarification regarding how this proposed change will be applied to low-impact entities. Currently low impact entities are not required to provide a discreet low impact inventory list and the proposed revision seems to contradict this.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	
Conceptually, the SRC agrees with what the SDT has proposed regarding the identification of SCI; however, we don't think the language is clear enough to implement in practice. **Recommendation:** Further clarify the definition to avoid inadvertent inclusion of systems supporting configuration management / monitoring that are not used to implement virtualization; i.e. sharing of computing resources.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
SCI does not present any more risk than EACMS. There is not a specific requirement to identify EACMS, PACS, or PCA in CIP-002. Similarly to EACMS, the association to the BCS is what brings the SCI into scope. SCI should be listed in applicable systems just like EACMS.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	

Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy believes if there is not a clear understand the concept of SCI and logical Isolation to properly classify Cyber Assets according to function and impact. Need “Logical Isolation” defined.	
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	
Same comments to question 11. CIP-002 is the bridge between cybersecurity and reliability function, the inclusion of SCI which is not directly implementing a reliability function does not seem related. Request explicit additional language for (EACMS, PACS, and PCAs) or (remove SCI, EACM, PACS, and PCAs addition). Auditors and entities need clarity on when EACMS, PACS, and PCAs are in scope. Request clarification on R1.5 (Medium Impact). It appears that adding SCI could bring more items into scope. Is that correct? Suggest reviewing the definition for better clarity. Suggest clarification on the analysis required for SCI, SCI/EACMS vs EACMS alone.	
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 SRC.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	

Comment
We disagree with the proposed changes. EACMS, PACS and PCAs are not included in the initial CIP-002 process; therefore, the SCI hosting EACMS PACS and PCAs should not be included in the initial CIP-002 process. We recommend revising R1.4 and R1.5as indicated below. **1.4.** Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above [delete: or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)] **1.5.** Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above [delete: or their associated EACMS, PACS or PCAs.]

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	

Comment
Concerns on the definitions caused this no vote for this standard. Concerned about the use of the term “assets” and the Technical Rationale that states an “asset containing” could be a location of a Management System used to manage a distributed SCI. The TR also includes “control centers” and not “Control Centers”. This could require the inclusion of locations other than the CIP-002 Assets and the location of the device used for electronic security controls, becomes part of the CIP program. Extrapolating this concept out, the entire SCADA system could become part of the program if a portion of it is a BCA. CIP-002 is the bridge between cyber security and reliability function, the inclusion of SCI which is not directly implementing a reliability function, does not seem related. Request explicit additional language for (EACMS, PACS and PCAs) or (remove SCI, EACM, PACS and PCAs addition). Auditors and entities needs clarity on when EACMS, PACS and PCAs are in scope

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports Marty Hostler and Northern California Power Agency comments.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	

Comment

The definition of Shared Cyber Infrastructure is open to multiple interpretations as written. The confusion is compounded by the exclusion of Shared Cyber Asset from the definition of Cyber Asset (Cyber Asset itself a problematic definition at times). The intent of the SDT is unclear preventing recommending an alternative proposal.

NERC, including the SDT, needs to be prepared and ensure that adequate CMEP SDT developed guidance is in place to broadly communicate the intent, implementation guidance, and interpretation of the new definitions on passage and prior to NERC Membership and our vendors beginning work to bring systems into compliance. In general terms, WVPA would have preferred that the SDT adopted the terms and directly adapted the definitions used by NIST in their documentation, such as NIST SP 800-125.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Same comments to question 11

CIP-002 is the bridge between cyber security and reliability function, the inclusion of SCI which is not directly implementing a reliability function, does not seem related. Request explicit additional language for (EACMS, PACS and PCAs) or (remove SCI, EACM, PACS and PCAs addition). Auditors and entities needs clarity on when EACMS, PACS and PCAs are in scope

Request clarification on R1.5 (Medium Impact). It appears that adding SCI could bring more items into scope. Is that correct?

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

BCSI requirements are sufficient as in CIP-004 and CIP-011. Entities are compliant and appropriate controls are available to secure BCSI in current version.

Shared storage housing active BCS data should not be allowed for mixed trust environments and introduces significant risk to the BES.

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The language that has been added R1.3, R1.4 and R1.5 is somewhat unclear. Is the intent to identify SCI that hosts BCS, EACMS, PACS, and PCAs, or is the intent to identify SCI that hosts BCS and to identify associated EACMS, PACs, and PCAs? It is not clear what the intent is from the currently proposed language. If the intent is only to identify systems hosted on SCI, then it continues to leave a gap in CIP-002. If the SDT wants to fix the holes in CIP-002, then it should be done correctly and not in pieces, which just compounds the issues. This should be done with a wider view to the breakdowns in how CIP-002 is written so that it improves the security objectives of CIP-002 and how the process of identification of BCS and applicable systems should be identified.

Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We disagree with these changes. Resulting from our comments for QUESTION 1, SCI is not required because our proposed modifications to the existing definitions can address this issue.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
More clarification is needed pertaining to what is in scope and what is not in scope?	

As we stated earlier, there is a storage array issue - since storage array wasn't directly impacting assets, this would massively impact Basin - goes against how we have been defining that. PACS on to the storage array - which by these new definitions, implication would need separate storage array for assets that are in scope. Inherent separations are there such as encryption. Need to clearly identify what is contained here.

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

Management Modules are excluded from the definition of SCI, but not explicitly addressed within CAs. The requirements all explicitly address Management Modules of SCI, but not CAs (which should be inherent due to the lack of exclusion in the CA definition). This could lead to entities to exclude required protections for Management Modules on CAs – while implicit within the CA, they are not called out explicitly like in the SCI. Potentially missed requirements would include those around patching, user accounts, logging, change management, etc.

Additionally, for Self-contained Applicaitons defintion:

The term ‘immutable’ may limit the scope of the definition. While the base image may be immutable in a real-time sense, the running container does have the ability to have its configuration changed on an ongoing basis (while still reverting to the image upon termination).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Suggest reviewing the definition for better clarity.

Suggest clarification on the analysis required for SCI, SCI/EACMS vs EACMS alone.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

While CHPD agrees with the identification of SCI, it does not agree with the identification of SCI that host EACMS and PACS unless a corresponding requirement for the identification of EACMS and PACS is created. See question 11.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment
We disagree with the proposed changes. EACMS, PACS and PCAs are not included in the initial CIP-002 process; therefore, the SCI hosting EACMS PACS and PCAs should not be included in the initial CIP-002 process. We recommend revising R1.4 and R1.5as indicated below. **1.4.** Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above [delete: or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)] **1.5.** Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above [delete: or their associated EACMS, PACS or PCAs.]

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	

Comment
Suggest reviewing the definition for better clarity. Suggest clarification on the analysis required for SCI, SCI/EACMS vs EACMS alone.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	

Comment
Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

We disagree with the proposed changes. EACMS, PACS and PCAs are not included in the initial CIP-002 process; therefore, the SCI hosting EACMS PACS and PCAs should not be included in the initial CIP-002 process. We recommend revising R1.4 and R1.5 as indicated below.

1.4. Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above [**delete: or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs**)]

1.5. Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above [**delete: or their associated EACMS, PACS or PCAs**.]

Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Comments: *Changes from CIP-002-5.1 to CIP-002-7 include new terminology and applicability, in alignment with virtualization. Part 1.3 was revised to include identification of assets that contain a "low impact BCS and SCI that hosts any portion of a low impact BCS." The new Parts 1.4 & 1.5 added to include identification of associated SCI used for high/med impact BCS, EACMS, PACS or PCA, respectively. Identification of SCI within CIP-002 does address some of the risks associated with virtual infrastructure. However, as with other standards/requirements, CIP-002-7 depends upon approved SCI terminology and other definitions associated with virtualization as a whole.*

Likes 0	
Dislikes 0	

Response	
Marty Hostler - Northern California Power Agency - 5	

Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG does not agree with the proposed changes. The inclusion of EACMS and PACS as part of the proposed CIP-002 R1.4 and R1.5 is not consistent with the purpose of CIP-002 as a whole. CIP-002 primarily focuses on BES Assets and BES Cyber Systems, not the associated systems. If the intent of these proposed changes is to require an inventory of EACMS, PACS, and PCAs for high and medium impact BCSs, NRG recommends this proposed requirement be moved from CIP-002 to CIP-007.	
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	
Comments: Our comments and recommendations about SCI in QUESTION 1 provides the basis that small modifications to existing definitions can meet the requirement.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	No
Document Name	
Comment	
This is a significant change to a foundational part of the CIP Standards. The SDT is proposing to modify the categorization process from a single step for each asset to a multiple step process of identifying BCS and then reviewing those BCS for associated SCI. Additionally, how does an entity perform this function for low impact SCI when they aren't required to develop a list of low impact BCS?	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
NRG does not agree with the proposed changes. The inclusion of EACMS and PACS as part of the proposed CIP-002 R1.4 and R1.5 is not consistent with the purpose of CIP-002 as a whole. CIP-002 primarily focuses on BES Assets and BES Cyber Systems, not the associated systems. If the intent of these proposed changes is to require an inventory of EACMS, PACS, and PCAs for high and medium impact BCSs, NRG recommends this proposed requirement be moved from CIP-002 to CIP-007.	
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: Our comments and recommendations about SCI in QUESTION 1 provides the basis that small modifications to existing definitions can meet the requirement.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC
Answer	No
Document Name	
Comment
SRP is requesting clarification of how the change affects low impact devices
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
This is a significant change to CIP asset accounting. We agree it is a necessary change to help account for virtualization assets. However, identification of SCI should be a result of association to BCS. TVA notes that the risk of a system is based on configuration rather than classification.
Likes 0	
Dislikes 0	
Response
Leonard Kula - Independent Electricity System Operator - 2
Answer	No
Document Name	
Comment
Likes 0	
Dislikes 0	
Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial_Comment_Form_01222021_SC FINAL.docx
Comment	
See attached file.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the identification of SCI in Parts 1.3, 1.4 and 1.5.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 10.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	

Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the approach for BCS and SCI.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	
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	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	

Comment	
Ameren agrees with and supports EEI's comments.	
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	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

AEP supports the identification of SCI in CIP-002 Requirement R1 Parts 1.3, 1.4, and 1.5.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	

Comment

GSOC supports the addition and notes the following comments for the SDT's review and consideration:

1. Although the requirements have been modified to be inclusive of SCI and other supporting assets, proposed revisions to the purpose still focus solely on BCS identification. This could lead to confusion and should be revised to comport with the proposed revisions to the requirements. Revisions to the purpose could be as follows:

To identify and categorize cyber systems, assets, and infrastructure for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those that could have on the reliable operation of the BES. Identification and categorization of these systems, assets, and SCI support appropriate protection against compromises that could lead to misoperation or instability in the BES.

2. The format and content utilized for the identification of SCI and associated assets varies between high/medium and low impact BCS. It is recommended that consistent formatting be utilized.

3. In the proposed revisions, it is unclear whether the addition of SCI and attendant systems are those associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….."

4. In the proposed revisions, it is unclear as to whether the intent is to include all of the newly identified assets in the responsible entity's CIP-002 list or whether it is simply an additional identification activity to facilitate overall compliance. Further, the phrasing of the new revisions creates ambiguity relative to what ancillary/supporting assets (EACMS, PACS, and PCAs) are being identified relative. Specifically, the requirements should make clear whether the assets to be identified are:

a. Only the EACMS, PACS, and PCAs associated with SCI;

b. Only the EACMS, PACS, and PCAs associated with BCS AND hosted in SCI;

c. Only the EACMS, PACS, and PCAs associated with BCS that are hosted in SCI;

d. All of the EACMS, PACS, and PCAs associated with BCAs and BCS.

For this reason, clarification is requested. As an example, a revision that reflects option (d) above is provided below.

1.4 Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or the Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs) associated with the high impact BCS identified in Part 1.1 above.

1.5. Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above or the EACMS, PACS or PCAs associated with the medium impact BCS identified in Part 1.2 above.

5. The VSLs have been revised to incorporate the associated SCI, but not to include the required identification of additional, ancillary assets that are now included in the requirements. Consistency is needed between the requirement verbiage and the VSL verbiage. It is recommended that the revisions to the VSLs be revised to reflect the entirety of the revisions proposed in the requirements or that they be revised to reflect “applicable systems” to avoid the potential for misalignment resulting from revisions.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA suggests that the CIP Senior Manager annually (15 months) review what is included in SCI similarly to reviewing the BCS list for CIP-002 and CIP-003 compliance.	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	

NERC should further clarify what it considers to be Shared Cyber Infrastructure. Additionally, we have a question: is an asset SCI only if it is shared between a non-CIP Applicable System and a CIP Applicable System?

We request clarification on SCI residing at non-BES Facility (for example a data center) which is not a BES asset per those identified in CIP-002 R1 (i) to (vi); need clarification on how we would identify that Facility.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees with the proposed changes.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5

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	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
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	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
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	
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	

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	
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	
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	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
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	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	
Comment	
The new R1.4 and R1.5 require the identification and categorization of SCI that hosts any portion BCS/EACMS/PACS/PCA. It is agreed that SCI hosting BCS shall be included such that that secure controls/requirements can be properly applied. However, SCI hosting EACMS/PCAS/PCA poses the same risk as the physical EACMS/PCAS/PCA which are not currently included in new CIP-002 requirements. Suggest clarifying that physical EACMS/PCAS/PCA are in scope of CIP-002 or removing the requirements of identifying SCI hosting EACMS/PACS/PCA.	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	

11. In the current enforceable standards, there are no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement. The SDT revised CIP-002 to include the identification of SCI associated with EACMS, PACS, and PCAs to help address this issue within the virtualization scope of the current SAR. The proposed requirement could reduce possible non-compliance to a single issue if a Responsible Entity fails to properly identify SCI associated with EACMS, PACS, or PCAs. Do you agree with the proposed changes? 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

Consider revising to include EACMS and PACS as associated systems in the Purpose for consistency. However, identification of EACMS, PACS, and PCAs should be a result of association to BCS.

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: Our SCI comments and recommendations in QUESTION 1 support the basis that existng requirements can be slightly modified to meet the SAR and requirments.

Currently there is a gap in CIP-002 that doesn't require responsible entities to identify EACMS, PACS and PCA, but that aspect is not addressed by this SAR. If SDT intended to resolve this gap, we suggest adding lanaguate to R1.4 in CIP-002-5.1 as follows:

"Identify EACMS, PACS and PCAs that are associated with the high and medium impact BCS."

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NRG does not agree with the proposed changes. Please see response to question 10.

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

Comments: Our SCI comments and recommendations in QUESTION 1 support the basis that existng requirements can be slightly modified to meet the SAR and requirments.

Currently there is a gap in CIP-002 that doesn't require responsible entities to identify EACMS, PACS and PCA, but that aspect is not addressed by this SAR. If SDT intended to resolve this gap, we suggest adding lanaguate to R1.4 in CIP-002-5.1 as follows:

"Identify EACMS, PACS and PCAs that are associated with the high and medium impact BCS."

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 agrees with the inclusion of SCI but disagrees with identifying an SCI's associated systems. CIP-002 is written and designed to identify and categorize systems that impact reliability functions using a bright line criteria. The associated systems, PCA, EACMs, and PACS, are systems used to support security functions that protect the BCS or SCI. The additions also cause confusion because the identification of physical EACMS, PACS, and PCAs was not addressed.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	
NRG does not agree with the proposed changes. Please see response to question 10.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Changes from CIP-002-5.1 to CIP-002-7 include new terminology and applicability, in alignment with virtualization. Part 1.3 was revised to include identification of assets that contain a "low impact BCS and SCI that hosts any portion of a low impact BCS." The new Parts 1.4 & 1.5 added to include identification of associated SCI used for high/med impact BCS, EACMS, PACS or PCA, respectively. It clarifies things to make identification of SCI explicit within CIP-002. However, as with other standards/requirements, CIP-002-7 depends upon approved SCI terminology and other definitions associated with virtualization as a whole. Approval of CIP-002-7 would be conditional, based upon approval of the entire suite of new standards associated with virtualization.	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
We disagree with the proposed changes. Virtual EACMS, PACS and PCAs should be identified the same way as physical EACMS, PACS and PCAs. We recommend a future SAR for CIP-002 to address this issue.	
Likes 0	
Dislikes 0	
Response	

Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	

Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
The idea of identifying EACMS, PACS, and PCAs at the level of CIP-002 is interesting, except the VRF should be adjusted to reflect the impact of the asset, i.e., BCS,BCA VRF high EACMS, PACS, and PCAs VRF medium. CIP-002 is based on functional impact on the grid, it’s not obvious to conclude the same impact on the functional impact. Suggest clarification on the requirements.	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We disagree with the proposed changes. Virtual EACMS, PACS and PCAs should be identified the same way as physical EACMS, PACS and PCAs. We recommend a future SAR for CIP-002 to address this issue.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	No
Document Name	
Comment	
While CHPD agrees that there is a concern with the current standards' lack of a requirement to identify EACMS, PACS, and PCAs, the identification of such is outside the scope of the SAR. CHPD believes the SDT should not create a two-tiered system where SCI based EACMS and PACS must comply with different requirements than physical ones that are not strictly virtualization based. Such a change should be part of a new SAR.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
We support the NPCC TFIST and RSC comments and submit the following additional comments: The idea of identifying EACMS, PACS, and PCAs at the level of CIP-002 is interesting, except the VRF should be adjusted to reflect the impact of the asset, i.e., BCS,BCA VRF high EACMS, PACS, and PCAs VRF medium. CIP-002 is based on functional impact on the grid, it's not obvious to conclude the same impact on the functional impact. Suggest clarification on the requirements.	

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

We disagree with these changes. Resulting from our comments for QUESTION 1, SCI is not required because our proposed modifications to the existing definitions can address this issue. Currently there is a gap in CIP-002 that doesn't require responsible entities to identify EACMS, PACS and PCA, but it is not addressed by this SAR. If SDT intended to resolve this gap, we suggest adding R1.4 to the CIP-002-5.1 as follows:

"Identify EACMS, PACS and PCAs that are associated with the high and medium impact BCS."

Likes 0	
Dislikes 0	

Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
The language that has been added R1.3, R1.4 and R1.5 is somewhat unclear. Is the intent to identify SCI that hosts BCS, EACMS, PACS, and PCAs, or the is the intent to identify SCI that hosts BCS and to identify associated EACMS, PACs, and PCAs? It is not clear what the intent is from the currently proposed language. If the intent is only to identify systems hosted on SCI, then it continues to leave a gap in CIP-002. If the SDT wants to fix the holes in CIP-002, then it should be done correctly and not in pieces, which just compounds the issues. This should be done with a wider view to the breakdowns in how CIP-002 is written so that it improves the security objectives of CIP-002 and how the process of identification of BCS and applicable systems should be identified.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
Based on comments above, these changes are confusing and detrimental to security.	
Likes 0	

Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Same comments to question 10 CIP-002 is the bridge between cyber security and reliability function, the inclusion of SCI which is not directly implementing a reliability function, does not seem related. Request explicit additional language for (EACMS, PACS and PCAs) or (remove SCI, EACM, PACS and PCAs addition). Auditors and entities needs clarity on when EACMS, PACS and PCAs are in scope Request clarification on R1.5 (Medium Impact). It appears that adding SCI could bring more items into scope. Is that correct?	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

As written, an entity could still be found noncompliant for all requirements applicable to a EACMS, PACS or PCA. This additional requirement seems to add another PNC but only if the EACMS, PACS or PCA is virtualized.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We disagree with the proposed changes. Virtual EACMS, PACS and PCAs should be identified the same way as physical EACMS, PACS and PCAs. We recommend a future SAR for CIP-002 to address this issue.

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 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
Same comments to question 10. CIP-002 is the bridge between cybersecurity and reliability function, the inclusion of SCI which is not directly implementing a reliability function does not seem related. Request explicit additional language for (EACMS, PACS, and PCAs) or (remove SCI, EACM, PACS, and PCAs addition). Auditors and entities need clarity on when EACMS, PACS, and PCAs are in scope. Request clarification on R1.5 (Medium Impact). It appears that adding SCI could bring more items into scope. Is that correct? The idea of identifying EACMS, PACS, and PCAs at the level of CIP-002 is interesting, except the VRF should be adjusted to reflect the impact of the asset, i.e., BCS, BCA VRF high EACMS, PACS, and PCAs VRF medium. CIP-002 is based on functional impact on the grid, it's not obvious to conclude the same impact on the functional impact. Suggest clarification on the requirements.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	

Comment
There appears to be a gap in CIP-002 which doesn't require responsible entities to identify EACMS, PACS and PCA. If SDT intended to resolve this gap, we suggest adding lanaguate to R1.4 in CIP-002-5.1 as follows: "Identify EACMS, PACS and PCAs that are associated with the high and medium impact BCS."

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	

Comment
Please see JEA coments, an individual response to my comment is not required.

Likes 0	

Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
SCI does not present any more risk than EACMS. There is not a specific requirement to identify EACMS, PACS, or PCA in CIP-002. Similarly to EACMS, the association to the BCS is what brings the SCI into scope. SCI should be listed in applicable systems just like EACMS.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	
Conceptually, the SRC supports what the SDT is attempting to do regarding the consolidation of requirements to identify EACMS, PACS and PCAs into a single requirement. CIP-002 should include requirement language specific to the identification of any necessary categories to support the use of the Applicable Systems specification throughout the rest of the CIP standards. To do otherwise introduces a potential gap in activity required to identify and protect critical infrastructure and the systems supporting such protection.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	

Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the proposed modifications. However, the proposed modification only seems to solve the problem for SCI and not existing issues with associated Cyber Assets. Duke Energy is concerned that the treatment of SCI in a manner not commensurate with other in-scope systems introduces discrepancies in enforcement methods that will present challenges in working with regions. The current SAR should be expanded to address inventories of all relevant devices.	
Likes 0	
Dislikes 0	

Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
The modifications could reduce possible non-compliance to a single issue.	
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 SDT's intent to tie a non-identification of EACMS, PACS, and PCAs to a single requirement; however, Southern questions the usefulness in performing this activity only on virtual versions of these assets hosted on SCI that are being proposed for addition to CIP-002-7. Would physical Cyber Assets performing EACMS, PACS, or PCA functions not be just as important to identify and include? If the challenge of also including physical Cyber Assets alongside virtual ones in CIP-002 is a result of the scoping of the existing virtualization SAR, then… well, that is a shame and a gap in the ROP that should be addressed.	
Likes 0	
Dislikes 0	

Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	

Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
In the proposed revisions, it is unclear as to whether the intent is to include all of the newly identified assets in the responsible entity's CIP-002 list or whether it is simply an additional identification activity to facilitate overall compliance. Further, the phrasing of the new revisions creates ambiguity relative to what ancillary/supporting assets (EACMS, PACS, and PCAs) are being identified relative. Specifically, the requirements should make clear whether the assets to be identified are: a. Only the EACMS, PACS, and PCAs associated with SCI; b. Only the EACMS, PACS, and PCAs associated with BCS AND hosted in SCI; c. Only the EACMS, PACS, and PCAs associated with BCS that are hosted in SCI; d. All of the EACMS, PACS, and PCAs associated with BCAs and BCS. For this reason, clarification is requested. As an example, a revision that reflects option (d) above is provided below. 1.4 Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or the Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs) associated with the high impact BCS identified in Part 1.1 above. 1.5. Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above or the EACMS, PACS or PCAs associated with the medium impact BCS identified in Part 1.2 above.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	

Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the revisions to CIP-002 that include the identification of SCI associated with EACMS, PACS, and PCAs.	
Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
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	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
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	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	
Comment	
Texas RE agrees with the proposed changes. Additionally, although not specifically related to virtualization, it recommends the identification of all EACMS, PACS, and PCAs be required. If the identification of EACMS, PACS, or PCAs is only required for SCI, there is still "*no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement*" for EACMS, PACS or PCAs not associated with SCI. Texas RE recommends the following language: • Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset; and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs). • Identify each of the medium impact BCS according to Attachment 1, Section 1, if any, at each asset; and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).	
Likes 0	
Dislikes 0	
Response	

Dan Zollner - Portland General Electric Co. - 3

Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the approach for the identification of SCI associated with EACMS, PACS, or PCA.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 11.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the revisions to CIP-002 that include the identification of SCI associated with EACMS, PACS, and PCAs.	
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	
Joshua Andersen - Salt River Project - 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	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
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	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
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	

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	
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	
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	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 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	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
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 Cantwell - Lower Colorado River Authority - 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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
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	
Susan Sosbe - Wabash Valley Power Association - 1,3	
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	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

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

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	
Document Name	

Comment

See comments in Q10

Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

12. The SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved Request for Interpretation (RFI) regarding "shared BES Cyber Systems." The SDT modified the criterion to reference each discrete shared BCS. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	

Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy believes changes should be made to Criterion 2.1 and 2.2	
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 SRC.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We agree with this change; however, the qualifier of “at a single plant location” should be added. 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units [insert: **at a single plant location**], the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Request clarification - could multiple virtualized Low Impact BCS sharing the same SCI make that SCI Medium Impact under Criterion 2.1?	
Likes 0	
Dislikes 0	

Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
The language needs to make it more clear that the individual BCS would have to be in support of the generating units that surpass the threshold. The language change doesn't seem to clarify the interpretation of the criteria over the previous language that was used.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	

Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
CIP-002 Attachment 1, Criterion 2.1 is poorly worded.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved: Management Module Management Systems Self-Contained Application	

Shared Cyber Infrastructure	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with this change; however, the qualifier of “at a single plant location” should be added. 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units [insert: **at a single plant location**], the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

We agree with this change; however, the qualifier of “at a single plant location” should be added.

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units [insert: **at a single plant location**], the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	No
Document Name	

Comment

Request clarification: could multiple virtualized low impact BCS sharing the same SCI make that SCI medium impact under R2.1.

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

Comments: We believe adding “discrete” in Criterion 2.1 does not resolve the clarification. Criterion 2.1 and 2.2 have the same issue regarding which shared BCS shoulde be identified as medium impact.

In our view, the focus should be on a totol loss of 1500MWs or 1000MVAR rather than the adverse impacts. If using adverse impact as the assessment basis, all BCS would be identified as the medium impact BCS. In addition, the “shared” wording should be removed since non-shared BCS could also result in a loss of 1500MW.

Recommendations:

Changes to the Criterion 2.1 and 2.2 to be:

- 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. An individual BCS for a group of generating units, that could, within 15 minutes result in a total loss of 1500 MW or more in a single Interconnection.

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: We believe adding “discrete” in Criterion 2.1 does not resolve the clarification. Criterion 2.1 and 2.2 have the same issue regarding which shared BCS shoulde be identified as medium impact.

In our view, the focus should be on a total loss of 1500MWs or 1000MVAR rather than the adverse impacts. If using adverse impact as the assessment basis, all BCS would be identified as the medium impact BCS. In addition, the “shared” wording should be removed since non-shared BCS could also result in a loss of 1500MW.

Recommend:

Changes to the Criterion 2.1 and 2.2 to be:

- 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. An individual BCS for a group of generating units, that could, within 15 minutes result in a total loss of 1500 MW or more in a single Interconnection.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the change made to CIP-002 Attachment 1, Criterion 2.1 to address the approved RFI regarding “shared BES Cyber Systems”.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 12.	
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	
Request clarification - could multiple virtualized Low Impact BCS sharing the same SCI make that SCI Medium Impact under Criterion 2.1? The syntax should be the same for Criterion 2.2. Criterion 2.1 is the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, The current Criterion 2.2 is the only BCS that meet this criterion are those shared BCS that could, within 15 minutes.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the inclusion of the earlier CIP-002-5.1a imterpertation into CIP-002, Attachment 1, Criteria 2.1.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE notes that Part 2.12 was not approved by FERC and needs to be adjusted to the language found in CIP-002-5.1a.	
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	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
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	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
LCRA believes that having the “each discrete” before “shared BES Cyber Systems” sounds contradictory and may lead to confusion.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

AEP supports the change made to CIP-002 Attachment 1, Criterion 2.1 to address “shared BES Cyber Systems”.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	Yes
Document Name	

Comment

LCRA believes that having the “each discrete” before “shared BES Cyber Systems” sounds contradictory and may lead to confusion.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed changes.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	Yes
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

The syntax should be the same for Criterion 2.2. and Criterion 2.1..

Criterion 2.1. is :

the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes,

The current Criterion 2.2 is :

The only BCS that meet this criterion are those shared BCS that could, within 15 minutes,

Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes

Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
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	
Yes, Southern supports this change to CIP-002-6, Att 1, Part 2.1 criteria.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP is requestiong futher definition, “each discrete shared” BCS mean within the standard.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

The added term "discrete" helps to clarify what should be taken into account to calculate the 15-minute impact.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees with the proposed modifications to align with a previously approved Request for Interpretation (RFI) regarding shared BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
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	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
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	
Susan Sosbe - Wabash Valley Power Association - 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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
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	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
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	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
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	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
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	
Anthony Jablonski - ReliabilityFirst - 10	
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	
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	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
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	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
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	

Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	
Document Name	
Comment	
The SRC defers to comment as this Criterion is not applicable to the ISO/RTO community.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
Please see comments submitted by the ISO/RTO Council Standards Review Committee.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	

Answer	
Document Name	
Comment	
Abstain, not applicable to medium impact.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	

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

13. The SDT made conforming changes to CIP-003 and CIP-004. Do you agree with the proposed changes? 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

TVA disagrees with the underlying changes that necessitate the conforming changes.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

SRP considers the attention given to virtualization feels over weighted compared to non-virtualized systems. This increases the burden on entities without virtualization to comb through the standards to find what is applicable.

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: Our comments and recommendations in QUESTION 1 address CIP-003 and CIP-004. Based on our proposed revision to the definition of IRA, we agree the applicable systems in CIP-004 should be changed from “medium impact BCS with ERC to “medium impact BCS with ERC or IRA.”

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
CIP-003 Attachment 1 states, “Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI.” Please verify the usage of and/or in this sentence. Could an entity have a plan for either the BCS or associated SCI or do they need a plan for both, if applicable? The intent is not difficult to infer, but the SDT could clarify the intent with revised 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	
Comments: Our comments and recommendations in QUESTION 1 address CIP-003 and CIP-004. Based on our proposed revision to the definition of IRA, we agree the applicable systems in CIP-004 should be changed from “medium impact BCS with ERC to “medium impact BCS with ERC or IRA.”	
Likes 0	
Dislikes 0	

Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Agreement depends upon approved SCI terminology and other definitions associated with virtualization as a whole and documented throughout our comments.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Suggest a definition of « the **system(s)** outside the asset containing low impact BES Cyber System(s)BCS » a requirement 3.1 section 3 of the attachment 1 in CIP-003.	
Likes 0	
Dislikes 0	
Response	

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

We agree with the conforming changes to CIP-003 and CIP-004 Standard language.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	No
Document Name	
Comment	

In relation to CIP-004 R2.1, the new definition of IRA and addition of IRA to this requirement will expand the scope to serially connected assets that have IRA, which has a significant impact due to the large number of BC Hydro assets which are Medium Impact without ERC.

BC Hydro SME team suggests that SDT either revise the IRA definition and include routing as suggested in our response to Question # 1, or restore the previous version of the standard for this requirement with newly added terms.

Likes 0	
Dislikes 0	
Response	

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

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Suggest reviewing the definition for better clarity.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CIP-003 and CIP-004

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure

CIP-004

Comment: The change to this requirement would include all of the Medium Impact BCS.

However, additional clarity is needed on the new terms to see how this requirement affects an entity's facility that contain Medium Impact BCS.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The term “system(s)” in R2, Atch. 1, sections 3.1 is unclear whether itvrefers only to Cyber Assets and Virtual Cyber Assets. Would this term also include SCI? Since the Technical Rationale for Atch 1 Section 3.1 is the only place that describes the term “system(s)”, future revisions of the Technical Rationale should retain the description if still applicable. For clarity, the term "system" should be defined in the language of the requirement itself if it is intended to be applicable only to this instance of the usage of the term.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

Current standards are sufficient and these changes are cosmetic. No changes to CIP-004 are required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Without further refinement to the requirements as discussed in answers to the other questions, it would be inappropriate to support this change to the applicability

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE is concerned security risks still exist for CIP-004-7 by not including PCAs in the applicable systems column specifically for R4 and R5.

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports TVA's comments.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions caused this no vote for this standard.

ESP is still included in CIP-003 R1.1.2 even though it is retired. Should be replaced with the new name of CIP-005.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We agree with the conforming changes to CIP-003 and CIP-004 Standard language. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Eenrgy belives changes the applicable systems should be “medium impact BCS with ERC or IRA.” for CIP-004.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	

Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
We don’t agree with adding IRA as it will bring into compliance more devices that were previously excluded.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Please see comments in response to Question No. 9 regarding exemptions 4.2.3.2 & 4.2.3.3.	
Likes 0	
Dislikes 0	
Response	
Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC	
Answer	No
Document Name	
Comment	

CIP-003 Attachment 1 states, “Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI.” Please verify the usage of ’or’ in this sentence. Could an entity have a plan for either the BCS or associated SCI or do they need a plan for both, if applicable? The intent is not difficult to infer, but the SDT could clarify the intent with revised language.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees with the conforming changes to CIP-003 and CIP-004.

Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Reclamation recommends changing the title of CIP-003-9 Attachment 1 From: Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI To: Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS and associated SCI	
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 supports the conforming changes made to CIP-003 and CIP-004 given that the SDT is able to adequately address our other comments contained herein.	
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 to CIP-003 and CIP-004.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments on the conforming changes to CIP-003 and CIP-004 for the SDT's review and consideration:

2. The introductory sentence for CIP-003, requirement R1 was revised to include "and associated SCI," however, the applicable bullets in the subset list still only address BCS. While not all topics are applicable to SCI, several are and, therefore, the singular reference to BCS in a sub-bullet could result in confusion and ambiguity relative to whether the policy should address SCI relative to that topic. For example, requirements R1.1.3 and R1.1.6 address topics that are also applicable to SCI, but include only references to BCS. The SDT should clarify as to whether content on these topics should address solely BCS or also SCI and give due consideration as to how these similarities and differences in treatment of BCS and SCI should be addressed in Requirement R1.

3. Requirement R1.1.2 in CIP-003 still refers to ESPs despite the proposal to retire the term included in this posting.

4. The proposed revisions include modifications to the titles of certain reliability standards, e.g., CIP-005 and CIP-010, and titles should be modified in others to reflect the expanded scopes (e.g., inclusion of SCI), e.g., CIP-006 and CIP-009. Several of the bullets included in requirement R1 do not reflect the revised titles. Accordingly, a quality check should be performed to ensure consistency between CIP-003 and the referenced CIP reliability standard's titles with conforming revisions proposed where necessary. Alternatively, the topics could be revised to ensure broader applicability.

5. In the proposed revisions for CIP-004, for applicable systems, it is unclear why the construct/format utilized differs between requirements, e.g., requirement R1 and R2, and whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI

or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….."

6. In the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

It seems unneccesary to call out SCI in applicable systems column of CIP-004 R1.1 as other associated systems are not called out in the awareness training. There does not appear to be any real value gained by adding this qualifier to this section.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment	
MPC supports comments submitted by Duke Energy.	
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 CIP-003 and CIP-004.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP generally supports the conforming changes made to CIP-003 and CIP-004, except for those concerns identified within our responses to Questions 1 and 9.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

AEPCO is signing on to ACES comments.

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

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

Issue 1:

The addition of “with IRA” to the Applicable Systems column in CIP-004 will add significant burden to authorize and revoke access to systems that were previously not required to be managed in this way under CIP-004. There are many instances of medium impact facilities that have their external communication limited to serial in order to limit risk, which had the added benefit of de-scoping many CIP Requirements (CIP-004 being one set).

Issue 2:

Tacoma Power noted the lack of Management Module inclusion in the Applicability column in CIP-004, and would like feedback from the SDT on whether this exclusion was intentional.

Issue 3:

Additionally, the Applicable Systems SCI references in CIP-004 R5 should be sub-bulleted. For example, “SCI hosting High Impact BCS or their associated EACMS or PACS” should be changed to “•EACMS” and “•PACS”.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
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	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-003 and CIP-004. PG&E does have concerns and supports the input provided by EEI.

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

Suggest reviewing the definition for better clarity.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb 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; - Douglas Webb

Answer	Yes
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 13.

Likes 0	

Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI generally supports the conforming changes made to CIP-003 and CIP-004, except for those concerns identified within our responses to Questions 1 and 9.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	Yes
Document Name	
Comment	
The SRC supports the conforming changes made to CIP-003 and CIP-004 with respect to the high impact provisions applicable to ISO/RTO functions.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
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	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
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	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
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	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
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	
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	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
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	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
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 Cantwell - Lower Colorado River Authority - 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	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
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, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
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	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	

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	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	

Response

14. The SDT modified the Applicable Systems column in CIP-006 to include SCI hosting PACs associated with Medium Impact BCS with ERC or IRA. The SDT made the proposed revisions to clarify the scope of requirements that apply when an entity implements serial IRA. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The changes appear to be appropriate as long as corrections are made to the SCI definition. In addition, please see comments in response to Question No. 9 regarding exemptions 4.2.3.2 & 4.2.3.3.	
Likes 0	
Dislikes 0	
Response	

Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	

Comment

R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	No
Document Name	

Comment

No we disagree. In fact we don't even understand the questions based on the reading of the standard. So what ever the drafting team was trying to communicate isn't being conveyed in the current draft. What is the risk that this change is trying to address? Additionally, we agree with submitted comments from Duke Energy regarding the mention of serial IRA.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Eenrgy belives changes the applicable systems should be “medium impact BCS with ERC or IRA.” for CIP-006 and suggests providing clatify to proposed language to provide consistent application.

Likes 0	
Dislikes 0	

Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI recognizes the clear linkage between SCI hosting PACs associated with Medium Impact BCS with ERC within CIP-006, but there seems to be a gap in that linkage for IRA. Presently, IRA is not mentioned within the language of proposed CIP-006-7 or the technical rationale. EEI requests clarification how serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to IRA. At the present time, the only references to serial IRA are within the Technical Rationale for Definitions (see IRA). For this reason, EEI is unable to support the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 14.	
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	
R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part.	
Likes 0	

Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	

Comment
We disagree with the proposed changes to CIP-006. The present changes do not reference IRA within the language of proposed CIP-006-7 or the Technical Rationale. We request clarification on how the serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to the IRA. Presently, only references to serial IRA are within the Technical Rationale for Definitions. Additionally, more information in the Technical Rationale is requested regarding the concept and procedural controls of SCI without ERC hosting Medium Impact BCS, as found in the Applicable Systems of R1 part 1.1.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	

Comment
Concerns on the definitions caused this no vote for this standard. Do not understand how the proposed changes in scope have any impact on serial IRA. This clarification of scope does not seem to be discussed in the Technical Rational for CIP-006.

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

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports TVA's comments.

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

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Without further refinement to the requirements as discussed in answers to the other questions, it would be inappropriate to support this change to the applicability

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI's 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	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP, in support of EEI's comments, recognizes the clear linkage between SCI hosting PACs associated with Medium Impact BCS with ERC within CIP-006, but there seems to be a gap in that linkage for IRA. Presently, IRA is not mentioned within the language of proposed CIP-006-7 or the Technical Rationale. AEP requests clarification on how serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to IRA. At the present time, the only references to serial IRA are within the Technical Rationale for Definitions (see IRA). For this reason, AEP is unable to support the proposed changes.	

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

“SCI hosting PACs associated with Medium Impact BCS with ERC or IRA” is not in the Applicable Systems column for any of the CIP-006 requirements. Otherwise, SIGE agrees that serial IRA should be in scope.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
“SCI hosting PACs associated with Medium Impact BCS with ERC or IRA” is not in the Applicable Systems column for any of the CIP-006 requirements. Otherwise, CEHE agrees that serial IRA should be in scope.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
More information is needed on storage requirements and scope needs to be defined. SCI considerations will dictate our agreement to this particular item.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Medium Impact BCS with ERC or IRA is not listed in the Applicable Systems column in CIP-006-7. The question does not reflect the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
We support the NPCC TFIST and RSC comments and submit the following additional comments: R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	No
Document Name	
Comment	
Similar to comments provided in our response to Question # 1, the change in the definition of IRA and the use of term “Medium Impact BCS with ERC or IRA” will result in a major scope increase and change for BC Hydro. BC Hydro SME team suggests that SDT either revise the IRA definition and include routing as suggested in our response to Question # 1, or restore the previous version of standard for this requirement with newly added terms.	

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We disagree with the proposed changes to CIP-006. The present changes do not reference IRA within the language of proposed CIP-006-7 or the Technical Rationale. We request clarification on how the serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to the IRA. Presently, only references to serial IRA are within the Technical Rationale for Definitions. Additionally, more information in the Technical Rationale is requested regarding the concept and procedural controls of SCI without ERC hosting Medium Impact BCS, as found in the Applicable Systems of R1 part 1.1.

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

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	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
We disagree with the proposed changes to CIP-006. The present changes do not reference IRA within the language of proposed CIP-006-7 or the Technical Rationale. We request clarification on how the serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to the IRA. Presently, only references to serial IRA are within the Technical Rationale for Definitions. Additionally, more information in the Technical Rationale	

is requested regarding the concept and procedural controls of SCI without ERC hosting Medium Impact BCS, as found in the Applicable Systems of R1 part 1.1.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG does not agree that the proposed revisions clarify the scope of requirements with respect to IRA. Specifically, none of the “Applicable Systems” columns throughout CIP-006 contain the verbiage, “IRA”.	
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 disagrees with the addition of “SCI hosting High Impact BCS or their associated EACMS or PCA” and “SCI with ERC hosting Medium Impact BCS or their associated EACMs or PCA” to the applicable systems for CIP-006 R1.6 and CIP-006 R1.7. These additions are in conflict with the requirements language that focuses on the protections to Physical Access Control Systems themselves.

Excerpt of Requirement Language for context.

CIP-006 R1.6 “Monitor each Physical Access Control System for unauthorized physical access to a **Physical Access Control System**.”

CIP-006 R1.7 “Issue an alarm or alert in response to detected unauthorized physical access to a **Physical Access Control System** to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.”

ISO-NE agrees with the addition of “SCI hosting PACS associated with High Impact BCS” and “SCI hosting PACS associated with Medium impact BCS with ERC” as this correctly reflects the intention of the requirements.

Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	No
Document Name	

Comment

No response, however refer to previous need for IRA change clarification

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

Comments: Our comments and recommendations in QUESTION 1 address CIP-006. Based on our proposed IRA revision, we believe the applicable systems in CIP-006 should be changed from medium impact BCS with ERC to “medium impact BCS with ERC or IRA.”

Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
The applicability section does not clarify the scope of requirements that apply when an entity implements serial IRA in CIP-006. It clearly defines the scope for BCS and SCI with ERC.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
NRG does not agree that the proposed revisions clarify the scope of requirements with respect to IRA. Specifically, none of the “Applicable Systems” columns throughout CIP-006 contain the verbiage, “IRA”.	
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: Our comments and recommendations in QUESTION 1 address CIP-006. Based on our proposed IRA revision, we believe the applicable systems in CIP-006 should be changed from medium impact BCS with ERC to “medium impact BCS with ERC or IRA.”	
Likes 1	Lincoln Electric System, 1, Johnson Josh

Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	

Comment
The undefined term "serial IRA" appears to be in conflict with the current definition of IRA supplied in the NERC Glossary of Terms. Remove "serial," or clarify what is meant by "serial IRA." The proposed language lacks the clarity to provide a consistent application.

Likes 0	
Dislikes 0	

Response

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

Comment
Duke Energy does not agree that the proposed modifications clarify the scope of requirements that apply when an entity implements serial IRA. There is no inclusion of IRA within the language of proposed CIP-006-7 or the technical rationale. Duke Energy recommends clarification as to how serial IRA are to be addressed within the framework of CIP-006-7.

Likes 0	
Dislikes 0	

Response

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

Comment

Likes 0	
Dislikes 0	

Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-006 to include SCI. PG&E does have concerns and supports the input provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC provides the following comments for the SDT's review and consideration: 7. It is recommended that the SDT evaluate whether revisions to the title and purpose of CIP-006 are necessary to ensure consistency with its expanded scope. 8. In the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
If the SDT specifically meant to address IRA, then it was not achieved. We do NOT see any reference to the term Interactive Remote Access or IRA in the proposed standard.	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Adding “SCI Hosting High Impact BCS” and “SCI with ERC Hosting Medium Impact BCS” is necessary to insure that the scope of the applicable systems includes any possible virtual systems.	
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 acknowledges the clear linkage between SCI hosting PACs associated with Medium Impact BCS with ERC within CIP-006, but there seems to be a typo in this question related to IRA. Presently, IRA is not mentioned within the language of proposed CIP-006-7, as a qualifier for any Applicable System, or mentioned in the Technical Rationale. Southern recommends clarification as to how the implementation of serial IRA is to be addressed within the framework of CIP-006-7. Otherwise, Southern supports the ability to place the physical underlay of SCI hosting PACS associated with h/m BCS with ERC inside a PSP to meet the requirement.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Agree, with the proposed change to clarify the scope of the requirements for applicable systems with ERC and without ERC, but none of the applicable systems in CIP-006 included any reference to IRA as the question suggests.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
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	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
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	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
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	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
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	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
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	
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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	

Answer	
Document Name	
Comment	
Conceptually, the SRC agrees with what the SDT is proposing to do; however, we defer to medium and low impact entities to comment on the proposed language.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	

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

15. The SDT made conforming changes to CIP-008 and CIP-009. Do you agree with the proposed changes? 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

TVA disagrees with the underlying changes that necessitate the conforming changes.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

SRP considers the attention given to virtualization feels over weighted compared to non-virtualized systems. This increases the burden on entities without virtualization to comb through the standards to find what is applicable.

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: Our comments and recommendations in QUESTION 1 address CIP-008 and CIP-009 regarding the new or modified definitions.

Likes 1	Lincoln Electric System, 1, Johnson Josh
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	
Comments: Our comments and recommendations in QUESTION 1 address CIP-008 and CIP-009 regarding the new or modified definitions.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Agreement depends upon approved SCI terminology and other definitions associated with virtualization as a whole and documented throughout our comments.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	

Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with the conforming changes to CIP-008 and CIP-009 in the Standard language. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Until more context (technical diagrams or examples of applicable cyber assets) is provided for the SCI definition.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	

Answer	No
Document Name	
Comment	
Agree with changes to CIP 009. For CIP 008, scope needs to be limited to only include devices that impact the BES.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Without further refinement to the requirements as discussed in answers to the other questions, it would be inappropriate to support this change to the applicability	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	

Comment	
FMPA supports TVA's comments.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We agree with the conforming changes to CIP-008 and CIP-009 in the Standard language. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	

Comment	
CPS Energy believes the attention given to virtualization feels over weighted compared to non-virtualized systems and may increase burden to entities.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The changes appear to be appropriate as long as corrections are made to the SCI definition. In addition, please see comments in response to Question No. 9 regarding exemptions 4.2.3.2 & 4.2.3.3.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	

Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees to the conforming changes to CIP-008 and CIP-009.	
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 supports the conforming changes made to CIP-008 and CIP-009 given that the SDT is able to adequately address our other comments contained herein.	
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 to CIP-008 and CIP-009.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Suggest reviewing the definition for better clarity.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	

Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
In the proposed revisions for CIP-008 and CIP-009, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these across the body of CIP reliability Standards along with attendant revisions for clarity are requested e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….." Further, in the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Suggest reviewing the definition for better clarity.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

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 CIP-008 and CIP-009.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	Yes
Document Name	

Comment

AEP generally supports the conforming changes made to CIP-008 and CIP-009, except for those concerns identified within our responses to Questions 1 and 9.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
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	
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 recommends that the SDT add a note in the CIP-008-7 technical rationale to capture definition changes to “Cyber Security Incident” and “Reportable Cyber Security Incident”.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Ameren agrees with and supports EEI's comments.

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

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	

Comment

Texas RE does not have comments on this 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.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-008 and CIP-006. PG&E does have concerns and supports the input provided by EEI.

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

Suggest reviewing the definition for better clarity.

Likes 0	

Dislikes 0	

Response

Douglas Webb - Douglas Webb 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; - Douglas Webb

Answer	Yes
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 15.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

EEI generally supports the conforming changes made to CIP-008 and CIP-009, except for those concerns identified within our responses to Questions 1 and 9.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Other than the concerns noted in our response to Question #9, the SRC supports the conforming changes made to CIP-008 and CIP-009.

Likes 0	
Dislikes 0	

Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
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	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
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	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
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	
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	
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	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 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	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
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 Cantwell - Lower Colorado River Authority - 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	
Payam Farahbakhsh - Hydro One Networks, Inc. - 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	
Susan Sosbe - Wabash Valley Power Association - 1,3	
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	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
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	

Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	
Document Name	

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	
Document Name	

Comment

Current standards are sufficient and these changes are cosmetic. No changes to CIP-008 or 009 are required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

Likes 0	
Dislikes 0	
Response	

16. The SDT modified CIP-011 Requirement R2 part 2.1, which will allow cryptographic erasure in scenarios where BCSI can't be mapped to particular disks in virtualized storage. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

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

The SRC agrees with combining Parts 2.1 and 2.2 under Requirement R2 and proposes to augment the proposed language by adding "that contain BCSI" as some BES Cyber Assets, such as PCA, may not contain BCSI at all.

Recommendation: Revise the Requirement in Part 2.1 as follows:

*Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems **that contain BCSI** prior to their disposal or reuse (except for reuse within other systems identified in the "Applicable Systems" column).*

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CIP-011 Part 2.1 does not mention cryptographic erasure. It is unclear what is meant by “cryptographic erasure.” It would be more appropriate for the SDT to directly address striping of data or other means that obfuscate information on disks in virtual storage. The second requirement is identified as R1. It should be R2.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

Although cryptographic erasure (CE) is utilized making the encrypted data impossible to decrypt, is it possible to recover data (BCSI) from the applicable system since there was no specifc data targeted? Additionally, consider revising the new part 2.1: “Method(s) to prevent the unauthorized

retrieval of BCSI from applicable systems that contain BCSI prior to upon their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column). “

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 correct label for R2. Currently shows R1 – immediately before M2 – on PDF page 9 of 18.

Request review of the column Applicable Systems, Management modules, and Management systems should be part of R1 and R2.

Request clarification in the requirement to allow cryptographic erasure, this mechanism should not be in the requirement, the requirement should stay at the high level. cryptographic erasure should me move to the Technical Rationale.

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 SRC.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No

Document Name	
Comment	
We agree with the proposed changes to CIP-011 R2 part 2.1. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP offers the following comment for the SDT consideration for Question 16: Recommend the SDT add clarity to the requirement or measure on the reuse of the physical storage location of virtual machine files being deleted or removed from the SCI. This could become problematic to machines that reside outside the ESP (EACMS and PACS).	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard.	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	

Answer	No
Document Name	
Comment	
FMPA supports TVA's comment: Consider revising to include a process to capture the encryption keys' management if using VMs/solid-state drives. The proposed language does not include the term "cryptographic erasure". The proposed language lacks the clarity to provide the consistent application.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
The Measures section stating “Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI” should be extended to allow escorted transport between physical security perimeters.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Request correct label for R2. Currently shows R1 – immediately before M2 – on PDF page 9 of 18	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	

Answer	No
Document Name	

Comment

Current standards are sufficient and these changes are cosmetic. No changes to CIP-007 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

Mixed trust environment should not be permitted for BCS.

BCSI requirements are sufficient as in CIP-004 and CIP-011. Entities are compliant and appropriate controls are available to secure BCSI in current version.

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based on security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Agree with SDT. If BCSI is not on the PCA, it should be identified as such because it would then not need to be protected. PCAs need to be included in to protect BCSI. Clarification in the guidance would be beneficial.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with the proposed changes to CIP-011 R2 part 2.1.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

For CIP-011-3 R2, the SDT consolidated former Parts 2.1 and 2.2 into a single requirement. Similar to R1, the applicability is expanded with conforming terminology that includes virtualization: "SCI hosting High or Medium Impact BCS or their associated: EACMS; PACS; or PCA."

Removal of Part 2.2 is a positive step that would allow Responsible Entities greater flexibility in dealing with sanitization of virtual systems. However, use of Cryptographic Erasure(CE) is complex and would require additional documentation for things such as key management and destruction records in order to demonstrate that the data is permanently irretrievable. In addition, all backup copies of the respective BCSI or BCS systems require destruction as well. This would need to be included in that standards to ensure that the entity has proper documentation to address the additional processes needed to address Cryptographic Erasure.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NRG requests additional clarity with respect to scenarios where cryptographic erasure is allowed. This language is not referenced in either the Requirements or Measures sections of CIP-011 R2.1 but appears to be implied by virtue of the proposed changes. Thus, more explanation is needed.

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

Comments: We agree with the combination of R2 part 2.1 and 2.2 as long as the language is further refined to address some CIP cyber assets such as PCA which may not contain BCSI at all.

Recommendations:

- We suggest retaining the language “contains BCSI” from the existing version, and consider the following wording for the new part 2.1:
    - “Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems that contain BCSI prior to upon their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column). “

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NRG requests additional clarity with respect to scenarios where cryptographic erasure is allowed. This language is not referenced in either the Requirements or Measures sections of CIP-011 R2.1 but appears to be implied by virtue of the proposed changes. Thus, more explanation is needed.

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: We agree with the combination of R2 part 2.1 and 2.2 as long as the language is further refined to address some CIP cyber assets such as PCA which may not contain BCSI at all.

Recommend:

- We suggest retaining the language “contains BCSI” from the existing version, and consider the following wording for the new part 2.1:

“Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems that contain BCSI prior to upon their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column). “

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
1. SRP is requesting a better description of what are the “allowing for cryptographic erasure in scenarios where BCSI cannot be mapped to particular disks within virtualized storage, and where BCSI is stored on SCI employing deduplication”. How would we perform an exercise for disposal an in Vitual world. Does cryptographic erasure need to be done on the virtual volume or in the physical storage? 2. SRP needs clarification on, “cryptographic erasure”. The term is not in the standard, only in the technical rationale. What does Virtual disposal look like? Please clarify what is necessary for evidence.

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 revising to include a process to capture the encryption keys' management if using VMs/solid-state drives. The proposed language does not include the term "cryptographic erasure". Proposed language lacks the clarity to provide consistent application.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes made to R2, Subpart 2.1, however, EEI suggests that adding language, similar to what is used within the Technical Rationale, to the Measures column of Table R2 – Reuse and Disposal, bullet 1 to clarify that “cryptographic erasure in scenarios where BCSI cannot be mapped to a particular disk in virtualization storage” is an acceptable measure for this requirement.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 16.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	

Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the modifications to CIP-011 R2, Part 2.1. PG&E also supports the input provided by EEI for this modification.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	

ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
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 noted the lack of Management Module inclusion in the Applicability column in CIP-011, and would like feedback from the SDT on whether this exclusion was intentional.	
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

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

Answer	Yes
Document Name	

Comment

AEPCO is signing on to ACES comments.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	Yes
Document Name	

Comment

AEP supports the proposed changes made to CIP-011 Requirement R2, Part 2.1.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

AZPS agrees with he proposed changes.

Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
We support the NPCC TFIST and RSC comments and submit the following additional comments: Request correct label for R2. Currently shows R1 – immediately before M2 – on PDF page 9 of 18 Request review of the column Applicable Systems, Management modules and Management systems should be part of R1 and R2.	

Request clarification in the requirement to allow cryptographic erasure, this mecanism should not be in the requirement, the requirement should stay at the high level. Cryptographic merasure should me move to the Technical Rationale.	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC provides the following comments for the SDT's review and consideration: 9. In the proposed revisions for CIP-011, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….." 10. In the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion. 11. A typographical error was identified in the form of duplicate R1s. It is suggested that the second R1 be revised to R2.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
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
We can’t say that we agree or disagree, it’s not really clear what the intent is or what is being accomplished with the changes other than to add sci to the applicability column. Not sure I understand how the modification specifically allows for cryptographic erasure. We agree that management modules should be excluded from this requirement as that presumes that the module contains BCSI; this might be a stretch.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes
Document Name	

Comment
Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment
Request correct label for R2. Currently shows R1 – immediately before M2 – on PDF page 9 of 18

Request review of the column Applicable Systems, Management modules and Management systems should be part of R1 and R2.

Request clarification in the requirement to allow cryptographic erasure, this mecanism should not be in the requirement, the requirement should stay at the high level. Cryptographic merasure should me move to the Technical Rationale.

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 to CIP-011 R2 part 2.1.

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 supports the proposed changes made to R2, Part 2.1, however, Southern requests that the SDT add language, similar to what is used within the Technical Rationale, to the Measures column of Table R2 – Reuse and Disposal, bullet 1 to clarify that “cryptographic erasure in scenarios where BCSI cannot be mapped to a particular disk in virtualization storage” is an acceptable measure for this requirement.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees to the proposed modifications as the proposed language is flexible in allowing multiple methods.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
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	

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	

Teresa Cantwell - Lower Colorado River Authority - 5	
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	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Adrian Andreoiu - BC Hydro and Power Authority - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
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	
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	
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	
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	
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	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
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	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
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	
Maggy Powell - Amazon Web Services - 7	
Answer	

Document Name	
Comment	
There is a typographical error on Page 9 where the requirement is labeled R1, but should say R2.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.	
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	

17. The SDT performed a review of the CIP Standards and determined that CIP Exceptional Circumstances could be applied to the following additional requirements: CIP-004-7 Requirement R2 Part 2.2, CIP-004-7 Requirement R3 Part 3.5, CIP-006-7 Requirement R1 Part 1.8, CIP-006-7 Requirement R1 Part 1.9, CIP-006-7 Requirement R2, CIP-010-5 Requirement Part 1.2, and CIP-010-5 Requirement R1 Part 1.3. Do you agree with the proposed changes? 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

Any place where CEC is added to the CIP requirements is desirable. It should be added to all CIP requirements, but it is understood that that is outside of this project's charter.

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

Response

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

Answer	No
Document Name	

Comment

Comments: We do not find issue with applying exceptions to the existing standards, however implementing separate and diverse exceptions approach for certain requirements/parts or sub-requirements can cause issues for entities processes for declaring, establishing, managing and closing an Exceptional Circumstance. Recommend finding a method to consolidate an Exceptional Circumstance into a single process language.

Likes 1	Lincoln Electric System, 1, Johnson Josh
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

Comments: We do not find issue with applying exceptions to the existing standards, however implementing separate and diverse exceptions approach for certain requirements/parts or sub-requirements can cause issues for entities processes for declaring, establishing, managing and closing an Exceptional Circumstance. Recommend finding a method to consolidate an Exceptional Circumstance into a single process language.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We agree with the addition of CIP Exceptional Circumstances to the listed standards and requirements; however, we recommend adding CIP Exceptional Circumstance to CIP-006 Requirement R1 Parts 1.2 – 1.9.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with the addition of CIP Exceptional Circumstances to the listed standards and requirements; however, we recommend adding CIP Exceptional Circumstance to CIP-006 Requirement R1 Parts 1.2 – 1.9.	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	No
Document Name	
Comment	
The parent requirement under CIP-006-7 R2 now includes “except during CIP Exceptional Circumstance” while the table seem to have removed “except during CIP Exceptional Circumstance” for Part 2.1. However, Part 2.2 has “except during CIP Exceptional Circumstance” included. The tables are used as our primary source of guidance and would be beneficial to have “except during CIP Exceptional Circumstance” in each of the applicable table(s).	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	

Comment	
Agree with the changes, but this should be part of a different SAR. These changes likely go beyond considerations for virtualization.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
Current standards are sufficient and these changes are cosmetic. No changes to CIP-007 are required to address Virtualization. Only applicability section needs to be modified along with BCS definition	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	

We do not find issue with applying exceptions to the existing standards, however implementing separate and diverse exceptions approach for certain requirements/parts or sub-requirements can cause issues for entities processes for declaring, establishing, managing, and closing an Exceptional Circumstance. Recommend finding a method to consolidate an Exceptional Circumstance into a single process language

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We agree with the addition of CIP Exceptional Circumstances to the listed standards and requirements; however, we recommend adding CIP Exceptional Circumstance to CIP-006 Requirement R1 Parts 1.2 – 1.9.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Energy would recommend a method to consolidate CIP Exceptional Circumstance into a simplified process to include required documentation and perhaps CIP Senior Manager approval.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CIP Exception Circumstance already applies to CIP-004 Part 2.2. The SDT should consider adding CIP Exceptional Circumstance language to CIP-007 Part 4.1. Does the SDT intend for CIP Exceptional Circumstance language to apply to all of CIP-010 Part 1.2 or only Part 1.2.1? Does the SDT intend for CIP Exceptional Circumstance language to apply to all of CIP-010 Part 1.3 or only Part 1.3.1?

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

{C}CIP-004-6 Requirement R2 Part 2.2 already includes CEC language. If the CEC language is already in CIP-006-7 Requirement R2 should it be removed from Part 2.2 as it was from Part 2.1?

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy agrees with the proposed modifications that CIP Exceptional Circumstances could be applied.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Reclamation supports the inclusion of CIP Exceptional Circumstances where applicable.

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
Yes, Southern supports the addition of CEC language in each of these requirement parts.
Likes 0	
Dislikes 0	
Response
Carl Pineault - Hydro-Qu?bec Production - 5
Answer	Yes
Document Name	
Comment
No comments
Likes 0	
Dislikes 0	
Response
Ryan Olson - Portland General Electric Co. - 5
Answer	Yes
Document Name	
Comment
Portland General Electric Company supports this change
Likes 0	
Dislikes 0	
Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes

Document Name	
Comment	
AZPS agrees with he proposed changes.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports these changes.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments, please see below: ACES agree with the SDT's changes to the above requirements, but if the SDT is adding CIP Exceptional Circumstances to various requirements, CIP-013 should also have an allowance for CIP Exceptional Circumstances for emergency procurements.	
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	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
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	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Texas RE proposes expanding the CIP Exceptional Circumstances exception to apply to all requirements. CIP Exceptional Circumstances can cover a variety of scenarios, may come at unexpected times, and may have unanticipated effects on a Registered Entity's ability to comply.

Additionally, Texas RE recommends CIP-003 be revised to require Registered Entities to report to their Regional Entities when compliance obligations have not been met due to a CIP Exceptional Circumstance. Texas RE believes that an approach similar to the COVID-19 self-logs in which entities report issues associated with CIP Exceptional Circumstances to the ERO within a prescribed amount of time. While the ERO may review these CIP Exceptional Circumstance log submissions, the expectation is that such submissions will be resolved without further enforcement action.

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 agree with the SDT's changes to the above requirements, but if the SDT is adding CIP Exceptional Circumstances to various requirements, CIP-013 should also have an allowance for CIP Exceptional Circumstances for emergency procurements.

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports these modifications.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 17.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports these changes.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	

Answer	Yes
Document Name	
Comment	
The SRC supports proposed changes to existing standards.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
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	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

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

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	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 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	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
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 Cantwell - Lower Colorado River Authority - 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	

Payam Farahbakhsh - Hydro One Networks, Inc. - 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	
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	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
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	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
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	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

18. Implementation Plan: The SDT proposes an Implementation Plan that makes the revised CIP Standards and definitions effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order. However, the implementation plan allows a Responsible Entity to elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. Do you agree with this proposal? If you think an alternate effective date is needed, please provide a detailed explanation of actions and time needed.

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	

Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
The proposed changes that impact the CIP standards require significant changes to entities compliance program and associated documentation. Perhaps a staggered implementation plan or implementation after the effective date.	
Likes 0	

Dislikes 0	

Response

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

Comment
EEI is concerned that, given the expansive changes proposed to accommodate virtualization, many entities will need additional time to implement changes. There is also a need for additional time because of the change from an asset-based approach to a systems-based approach. For many entities, this will require significant training and process modifications, as well as significant changes to existing compliance and asset management tools. While we appreciate the efforts being made to minimize entity impacts, even with those efforts, the industry will be faced with significant challenges and some naturally unexpected hurdles to ensure companies are adequately prepared. For this reason, we do not support a 24-month Implementation Plan but instead recommend the implementation of these change occur in a phased approach similar to the implementation for CIP Version 5

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb 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; - Douglas Webb	
Answer	No
Document Name	

Comment
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 18,

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

Will the Implementation Plan be updated? Currently shows CIP-012-1 as part of this project. We understand this project is not updating CIP-012. That CIP-012's initial mandatory date has not changed.

How will entities notify their Region? This question comes from the section titled "Compliance Dates for Early Adoption of Revised CIP Standards and Definitions." This section says "In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the Revised CIP Standards and Definitions."

Can the Rules of Procedure be modified to allow phased implementation by the mandatory date?

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

Given the extensive impact of the proposed changes to accommodate virtualization, an implementation timeline cannot be determined until the draft standards are closer to final.

When considering an implementation timeframe, we request the SDT consider the burden the new applicable systems, definitions and technology implementations will have to our current CIPv5 programs. There will be significant administrative burden to adjust documentation to accommodate the changes, as well as to revise programs and processes for requirements that are not backward compatible.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerned about the requirement for the entity to notify the region when adopting early. This process would force the entity to do an action but not force the Regions to facilitate the action. It does not seem that the notification would impact the CMEP. Does the entity have to adopt all of the Standards at one time or can this be phased in? Would notification be required as each portion of a phased implementation is completed? Suggest deletion of the requirement to notify regions.

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	
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	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Will the Implementation Plan be updated? Currently shows CIP-012-1 as part of this project. We understand this project is not updating CIP-012. That CIP-012's initial mandatory date has not changed How will entities notify their Region? This question comes from the section titled "Compliance Dates for Early Adoption of Revised CIP Standards and Definitions." This section says "In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the Revised CIP Standards and Definitions."	

Can the Rules of Procedure be modified to allow phased implementation by the mandatory date?	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI's 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	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS believes the time would be spent on adhering to the new defnitions proposed and the program changes associated with them, and therefore would request a longer timeframe for the effective date. AZPS recommends 6 additional month totalling 30 months.	

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

Oklahoma Gas and Electric supports the comments provided by EEI.

Likes 0	
Dislikes 0	

Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
More clarity needs to surround the Glossary of Terms before these standards go into place.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	No
Document Name	
Comment	
BC Hydro SME team’s preliminary impact assessment of the required changes based on the current CIP Standards’ drafts estimates that more than 36 months would be needed to fully implement these changes. SDT is requested to consider this when formulating the effective date of implementation for entities.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Given the extensive impact of the proposed changes to accommodate virtualization, an implementation timeline cannot be determined until the draft standards are closer to final.	

When considering an implementation timeframe, we request the SDT consider the burden the new applicable systems, definitions and technology implementations will have to our current CIPv5 programs. There will be significant administrative burden to adjust documentation to accommodate the changes, as well as to revise programs and processes for requirements that are not backward compatible.

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

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

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Given the extensive impact of the proposed changes to accommodate virtualization, an implementation timeline cannot be determined until the draft standards are closer to final. When considering an implementation timeframe, we request the SDT consider the burden the new applicable systems, definitions and technology implementations will have to our current CIPv5 programs. There will be significant administrative burden to adjust documentation to accommodate the changes, as well as to revise programs and processes for requirements that are not backward compatible.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response 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	

Comments: Due to the extent of the changes to entities' existing compliance programs and associated documentation we would request a staggered implementation plan or at least 1 audit cycle – 3 years. We do not see the backward compatibility which was communicated early in the project.

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: Due to the extent of the changes to entities' existing compliance programs and associated documentation we would request a staggered implementation plan or at least 1 audit cycle – 3 years. We do not see the backward compatibility which was communicated early in the project.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

TVA does not consider 24 months a sufficient amount of time to implement given the issues identified.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy recommends an implementation plan of 48 months with early-adoption options. In particular, the changes to CIP-005 will need to be implemented in a deliberate manner that does not disrupt reliable BES operations. These changes potentially require entities to make significant changes to management network architecture. Entities cannot prudently make significant investment associated with these changes until after FERC approval is obtained, so a longer period after the approval date is necessary for this standard than would be required for changes where FERC's intent to approve is clearer.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

The SRC supports the proposed 24-month Implementation Plan (as a minimum) and the added flexibility for entities to transition to the revised standards and definitions prior to the effective date should they choose to do so. This assumes the SDT addresses the concerns raised in response to Question #1 concerning backward compatibility. Left unaddressed, SRC is concerned that entities may be required to expend significant administrative effort, akin to the level required in transitioning from V3 to V5, to modify existing program documentation merely to maintain status quo; i.e. to continue to comply with CIP standards absent any changes to adopt virtualization.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

The changes proposed will have significant impact on existing CIP programs in order to implement changes to configuration management systems, documentation, and possibly architecture. 24 months is the minimum that should be allowed to accommodate these changes.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the 24 month Implementation Plan.

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	Yes

Document Name	
Comment	
FMPA supports a 24 months implementation plan.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
LCRA recommends that the NERC Evidence Request Tool is released immediately following FERC Board of approval. This tool may aide in the implementation of these revised standards.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

AEP supports the 24-month implementation plan.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	Yes
Document Name	

Comment

LCRA recommends that the NERC Evidence Request Tool is released immediately following FERC Board of approval. This tool may aide in the implementation of these revised standards.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	Yes
Document Name	

Comment

No comments

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

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

Yes, Southern supports the proposed Implementation Plan. Given the backwards compatibility of the proposed revisions, Southern appreciated the SDT's efforts to ensure entities can choose the ways and means that best suit their own internal implementation timelines when moving from existing physical architectures to a more virtualized CIP environment.

Likes 0	
Dislikes 0	

Response

Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
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	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	

Comment	
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	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

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	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
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	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
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	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
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	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
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	
Anthony Jablonski - ReliabilityFirst - 10	
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	
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	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
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	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
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	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
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	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	

Please see comments submitted by the Edison Electric Institute	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	

19. Please provide any additional comments for the SDT to consider, if desired.

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	

Comment

In addition to the above comments, Duke Energy recommends the following:

The proposed applicability of CIP-005 R1 component parts to EACMS and PACS, and in particular Part 1.5, is a major expansion of scope reminiscent of the “spaghetti requirements” – although it is appropriate to apply these protections to SCI, applying them to virtual EACMS and PACS is excessive in comparison to existing EACMS and PACS requirements.

The revised standards introduces multiple anti-affinity requirements that will increase the number of physical hosts required in clusters to maintain cluster reliability and compliance. Duke Energy agrees that it is reasonable to separate Intermediate Systems given their specific risks and functions as the “bastion host,” but requiring additional “trust levels” that separate BCA, Management Systems, other EACMS like Logging solutions, etc. within the virtual environment will add significant cost and complexity without commensurate cybersecurity benefits. Separating IS from other systems should provide a adequate, cost-justified level of separation based on the security requirements applied to those other systems hosted on SCI.

The inclusion of SCI in the PACS Maintenance and Testing requirements (CIP-006 R3) does not appear to be necessary or make practical sense. This requirement is clearly aimed at maintaining the integrity of the Physical Security Perimeter. Including the local badge controller portion of the PACS is technically sound, but the inclusion of the PACS server in current requirments was already confusing and required clarity in the G&TB. Now, the addition of SCI further exacerbates the question of what it means to test the PACS. What should be performed on SCI to meet this requirement? Even tests of provisioning and deprovisioning access that can reasonably include the PACS application servers cannot be applied to the SCI portion of the Applicable Systems. We suggest that the SDT use this opportunity to clarify that the scope of this requirement is the PACS components themselves (i.e. local controllers, application software) and remove the broader systems from the requirements’ applicability. At minimum, the SDT must provide clarity in the requirement as to what portion of the testing would apply to SCI.

Overall, the SDT’s approach solves certain problems with Virtualization, but in doing so, creates discrepancies in how the standards are applied between traditional and newer technologies. The creation of additional “device types” while not resolving the overall inconsistency in treatment of devices (e.g. CIP-002 now addressing BCS and SCI but not EACMS and PACS, applying requirements to PACS hosted on SCI but not those hosted on Cyber Assets) may confuse entities and auditors. Duke Energy recommends that the SAR be adjusted as needed to ensure the revisions produce a coherent approach to compliance, or that the SDT confine their changes to be more consistent with the existing defined terminology.

Likes 0	
Dislikes 0	

Response

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

Comment

TVA welcomes changes to the standards that support innovation and increase security and reliability. However, the standards and supporting definitions as proposed lack sufficient clarity for effective implementation.

TVA supports an approach that embraces innovative technologies that enhance security and reliability. The proposed changes are myopic in requiring differentiation in virtualization technologies supporting compute, network, and storage resources. These distinctions are becoming increasingly indistinguishable as virtualization technologies evolve. Modern standards should make no distinctions in the treatment thereof, so as not to preclude adoption of emergent technology.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Comments:

The proposed changes would impact nearly all CIP standards. Edits to Applicability, for example, exceeds 170 changes. We believe the existing standard requirements could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, reduce the impact to entities' programs, and provide greater clarity to auditors.

Categorization: A virtual hardware platform operating multiple hosts including CIP and non-CIP hosts can be categorized as a single CIP Cyber Asset using the highest high water mark or with the multiple classifications. This clarifies compliance controls as technologies advance and operating systems, applications and components whether disks, arrays, solid state or chipsets. Once the virtual hardware platform operating multiple hosts are protected as the highest water marked CIP Cyber Asset, the CIP and non-CIP hosts can operate on the same hardware platform unless they share the CPU and memory.

Security Controls: The current CIP requirements for physical security, electronic access (authorization, authentication and accounting), software patch management, antimalware, vulnerability management, monitoring and logging, hardening, change and configuration management and supply chain establish security controls which prevent hosts within a hardware platform (virtual) from unauthorized communication or access to each. OSI layer 2 controls prevent communications ingress/egress each other (non-routed) on the hardware platform and virtual switch backplane.

Communications ingress/egress between the hardware platform (virtual server) hosts and non-hardware platform occurs at the OSI layer 3 and 4 via a routed protocol and identified EAP using the current language. This perspective allows an entity to use virtual hardware platforms independent of hosts categorizations.

Entities may not prefer to consolidate all hosts because of heightened risk (i.e. it puts many "eggs" in one basket) to the entire platform and/or system functions.

Using existing language and minor changes can give entities the flexibility to use virtual technologies. Virtual environments should contain differing levels of security within them. All physical Cyber Assets associated with a virtual environment, and associated software, should be high watermarked to the most secure classification.

The impacts to entities with the proposed changes are broad and deep. We recommend the SDT look to using existing language and concepts to address virtualization.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Comments:

The proposed changes would impact nearly all CIP standards. Edits to Applicability, for example, exceeds 170 changes. We believe the existing standard requirements could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, reduce the impact to entities' programs, and provide greater clarity to auditors.

Categorization: A virtual hardware platform operating multiple hosts including CIP and non-CIP hosts can be categorized as a single CIP Cyber Asset using the highest high water mark or with the multiple classifications. This clarifies compliance controls as technologies advance and operating systems, applications and components whether disks, arrays, solid state or chipsets. Once the virtual hardware platform operating multiple hosts are protected as the highest water marked CIP Cyber Asset, the CIP and non-CIP hosts can operate on the same hardware platform unless they share the CPU and memory.

Security Controls: The current CIP requirements for physical security, electronic access (authorization, authentication and accounting), software patch management, antimalware, vulnerability management, monitoring and logging, hardening, change and configuration management and supply chain establish security controls which prevent hosts within a hardware platform (virtual) from unauthorized communication or access to each. OSI layer 2 controls prevent communications ingress/egress each other (non-routed) on the hardware platform and virtual switch backplane.

Communications ingress/egress between the hardware platform (virtual server) hosts and non-hardware platform occurs at the OSI layer 3 and 4 via a routed protocol and identified EAP using the current language. This perspective allows an entity to use virtual hardware platforms independent of hosts categorizations.

Entities may not prefer to consolidate all hosts because of heightened risk (i.e. it puts many "eggs" in one basket) to the entire platform and/or system functions.

Using existing language and minor changes can give entities the flexibility to use virtual technologies. Virtual environments should contain differing levels of security within them. All physical Cyber Assets associated with a virtual environment, and associated software, should be high watermarked to the most secure classification.

The impacts to entities with the proposed changes are broad and deep. We recommend the SDT look to using existing language and concepts to address virtualization.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	
Document Name	
Comment	
Please define the term “System Hardening”.	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	
Document Name	
Comment	
In our assessment, the risk of sharing infrastructure across different security zones (BES Cyber Systems vs. non-BES Cyber Systems) is higher than the benefit gained from such virtualization. Con Edison and Orange & Rockland Utilities fully concur on the benefits of virtualizing within same ‘level’ security zones, but entities should not be virtualizing across trusted to untrusted security zones. We do not believe it is appropriate for SCI to be share across BES Cyber Systems and non-BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
Reclamation recommends that improved resilience or reliability of the BES be the primary consideration before an entity adopts any new or emerging technologies for BES reliability operating services.	

Reclamation also recommends utilizing existing FedRAMP criteria and air gapping Industrial Control Systems where possible from external communications.

Remove language in the new definitions and in any Requirement that refers to a third person (their).

Reclamation understands the driver for this round of comments, and requests that the SDT submit smaller packets of data for future rounds of commenting and balloting. This was a heavy lift for a resource-constrained entity to review with the depth and seriousness warranted.

Reclamation appreciates SDT efforts to incorporate NIST Framework into the NERC Standards and encourages the SDT to continue this practice moving forward by ensuring that requirements are not duplicated within the NERC Standards where they may overlap NIST Framework.

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

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

ISO-NE believes that the SDT's approach solves certain problems with virtualization. However, as mentioned in earlier comments, it also creates increased complexity and discrepancies in how the definitions and requirements are applied. Because of the new definitions, there is a mixing/matching of virtual and physical systems. The creation of additional "device types" while not resolving the overall inconsistency in treatment of devices may confuse both Registered Entities and auditors. ISO-NE recommends that the SDT consider the suggestions presented in the comments above, as well as carefully review and adjust the "Applicable Systems" column for consistency and to limit confusion across all CIP Standards.

Furthermore, ISO-NE recommends the added language in CIP-010 R3.2, "...that minimizes difference with the production environment…" be deleted because CIP-010 Part 3.3.2 requires that the differences between the test environment and production environment be documented.

ISO-NE appreciates the opportunity to comment.

Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	
Document Name	
Comment	
NRG requests that the Guidelines and Technical Basis sections be added back in instances where they were removed. Furthermore, NRG believes that examples in the Guideline and Technical Basis would prove helpful in instances where significant changes were made (i.e. diagrams depicting logical isolation for SCI, examples of management modules, etc.).	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
See Response to Question 1.	
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	
Under CIP-005-8 R1.5, Southern requests the SDT consider the following changes to the proposed edits to specify IP “network” communications:	

Detect known or suspected malicious Internet Protocol (IP) ***network*** *communications for both inbound and outbound* ***network*** *communications entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.*

Additionally, under CIP-005-8 R1.5, the proposed revisions to remove EAPs associated with high BCS and mediums at Control Centers and add PACS and EACMS hosted on SCI significantly increases the scope and adds requirements previously not applicable to those Applicable Systems. As with our previous comment, the use of the conjunctions “and” and “or” when referring to “and their associated:” is not used here consistently; this further supports our comments that applying these new requirements to PACS and EACMS should only apply when those systems are “hosted on the same SCI as a h/m BCS”, and are not justified from a risk-based perspective when simply considering stand-alone virtual PACS or EACMS that are not hosted on the same SCI as a h/m BCS.

Although there was no question related to conforming changes for CIP-013-3, Southern supports the conforming change edits to CIP-013-3 given that the SDT is able to adequately address our other comments contained herein.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Management Systems for non-virtual environments should be protected at the same level as the Management Systems for SCI; we understand that the SAR limited the SDT. Likely this could be captured by FERC as a conditional approval item for the next version of CIP Standards.

Please keep ESP and EAP as NERC Glossary terms. This may avoid future auditor interpretation issues and allow consistent application of the concepts across industry. It also helps preserve backward compatibility.

Please provide a draft copy of the NERC CIP ERT for the new requirements with the next posting. This would help entities assess the impacts the proposed changes would have to managing audit preparation under the new requirements.

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

Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	
Document Name	

Comment
No other comments

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	
Document Name	

Comment
GSOC respectfully provides the following general comments: 1. Relative to VSLs, the proposed revisions inconsistently refer to the assets more explicitly, e.g., BCS, SCI, etc., in some instances while utilizing Applicable Systems in other instances. Consistency is recommended in the drafting and development of VSLs. Further, to reduce the potential for error, it is recommended that the term “applicable systems” be utilized whenever possible. 2. Relative to titles and purpose, GSOC noted several titles and purpose with proposed revisions as well as those that did not have proposed revisions despite revisions that broadened their overall scope and applicability. To ensure consistency amongst the reliability standards and with the broader scope of applicable systems, GSOC recommends that these be evaluated holistically to identify the need for any additional conforming revisions. 3. Generally, the formatting of applicable systems within the applicable systems column should be evaluated for consistency of format. 4. In the proposed revisions, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on

these along with attendant revisions for clarity are requested, e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….."

5. In the applicable systems column, scoping of applicable systems with additional terms such as ERC, IRA, etc. seems to be inconsistently applied. While it is understood that these scope additions better tailor the requirements, inconsistent application and use of scoping verbiage can lead to ambiguity and confusion. For this reason, review of these scope additions and use of consistent scoping of verbiage is recommended.

6. Relative to CIP-013, which had conforming revisions only, GSOC provides the following comments for the SDT's review and consideration:

a. In the proposed revisions for CIP-013, , it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….."

b. The verbiage utilized in the VSLs differs from the verbiage utilized in the requirements and raises a questions as to whether the EACMS and PACS of SCI are in scope for the standard.

c. A typographical error was identified in requirement R1. Controlling should be revised to Control.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

Management Systems for non-virtual environments should be protected at the same level as the Management Systems for SCI; we understand that the SAR limited the SDT. Likely this could be captured by FERC as a conditional approval item for the next version of CIP Standards.

Please keep ESP and EAP as NERC Glossary terms. This may avoid future auditor interpretation issues and allow consistent application of the concepts across industry. It also helps preserve backward compatibility.

Please provide a draft copy of the NERC CIP ERT for the new requirements with the next posting. This would help entities assess the impacts the proposed changes would have to managing audit preparationunder the new requirements.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for details.

Likes 0	

Dislikes 0	

Response

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

Comment
The CPU and memory isolation language in the PCA definition, CIP-005 R1.2, and CIP-005 R2.6 are a poison pill to this draft. They create a 4-tier structure to virtualization; BCAs/PCAs, Management Systems, Intermediate Systems, and all other VMs. On a non-CIP system, such VMs could be hosted on a 4-node cluster and have suitable redundancy. Under the draft standards, none of these classifications can share CPU or memory with any other classification. This represents a potential doubling and possibly more of the infrastructure required, as you would need to have at least 2 hosts for BCA/PCA, 2 hosts for Management Systems, 2 hosts for Intermediate systems, and 2 hosts for other systems (for total of at least 8, with the potential for more given TOP-001 redundancy requirements), along with vastly increased complexity to prevent VMs of different classifications from running on the same host. This added complexity introduces risk, where a failure could render BCA unable to find an appropriate host to run, even when plenty of resources are available. All this cost and complexity is added to mitigate vulnerabilities that do not exist yet and are only theoretical (that is, a side channel remote execution or privilege escalation that crosses VM boundaries). The cited side channel attack by the SDT (row hammer) has not been seen in the wild and has not been shown to allow VM escape. Possibly one of these isolation requirements would be acceptable, but 3 separete ones make this untenable. Furthermore, these threats are already covered by two other CIP requirements. In the event that such vulnerabilities were discovered, either patches would be released that could be applied as required by CIP-007 R2 (or if the patches cannot be installed, a mitigation employed), or an entity would identify the vulnerability in their CIP-010 R3 vulnerability assessment and mitigate them as part of their action plan. With these proposed requirements, the SDT cripples the ability for entities to implement virtualization at all, essentially cutting off one’s hand to prevent getting a splinter. These CPU/memory isolation requirements place virtualization out of the reach of smaller entities and greatly eliminate the benefits for even larger entities. Approval of this draft would require entities who have already implemented virtualization to completely rearchitect their systems, or potentially scrap their virtual infrastructure all together due to the added burden. It also mandates a specific control to address a concern (isolate VMs), rather than addressing the underlying need (mitigate side-channel vulnerabilities), which is counter to the SDT’s stated goal of not requiring the “how” but requiring the “what”. If the SDT wishes to address side-channel vulnerabilities, it should do so in a separate SAR that looks at how entities address vulnerabilities (similar to a previous draft that combined CIP-007 R2 and CIP-010 R3). We believe these changes introduce a poison pill to the new draft which significantly increases the likelihood of rejection by industry.

Likes 0	
Dislikes 0	

Response

Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	
Document Name	

Comment
Entergy is concerned by the wholesale deletion of the Guidelines & Technical Basis section of each standard addressed by this revision. These sections provided valuable guidance and information used to develop and document compliance positions or interpretations. The loss of this information would increase ambiguity with the standards and potentially call into question long standing compliance interpretations. Entergy does not support the deletion of this information.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	
Document Name	

Comment
Similar to CIP-005-8, CIP-007-7 and CIP-010-5 Draft 1 versions, BC Hydro recommends that a reference to the Technical Rationale documents be included within the Associated Documents section of the Standard.

Likes 0	
Dislikes 0	

Response

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

Comment
Suggest not to include PACS and EACMS in the scope in the context of SCI as this requirement doesn’t exist for a PACS and EACMS not on a SCI. SAR is for including the virilization concepts not to add additional controls. Suggest reviewing the Applicable Systems of the different CIP associated to management modules. The current langage only refers to a Management Modules of SCI hosting. What about a the management module of a BCA ? Management Modules of SCI hosting would have more controls than a Management Modules of BCA. The SDT should look into the CMEP Practice Guides published on the NERC web site. The following documents; CMEP Practice Guide Virtual Systems, CMEP Practice Guide Virtual Network, CMEP Practice Guide Virtual Storage are pertaining to the virtualization and they contain enough elements for us to understand what needs to be done to be compliant. Those CMEP documents permit the usage of the virtualization with the current concepts and definitions. The SDT should use those documents and update the different CIPs documents with the required and corresponding wording.

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. TFEs required "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

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6

Answer	
Document Name	

Comment

Please consider how these virtualization standards apply to the cloud. The SDT stated that this is not intended for cloud implement; is this defined in the standards? These changes could contradict or be overly restrictive based on previous NERC guidance on BCSI in the cloud.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	Project 2016 Q19 response.docx

Comment
See the attached file.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	
Document Name	

Comment
See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	
Document Name	

Comment
It seems as though there are some inconcistencies within the applicable systems column throughout the standards. Is that the intent of the SDT? For instance, the applicable systems column in CIP-005 R1.1 contains PCAs and PACs and EACMS hosted on SCI. However, thoughout most of the other standards, the requirements list SCI hosting High or Medium Impact BCS with the associate PACS, PCS, and EACMS. There are several things that are not completely clear in this approach. It is unclear what the purpose of the phrase “hosted on SCI” is associated with PACS and EACMS. Would the requirement not apply if the PACS or EACMS is hosted on SCI or not in the CIP-005 R1.1? Based on the requirement language, it seems as though it shouldn’t matter whether they are hosted on SCI or not. Further clarification is needed around the intent of either the phrase “hosted on SCI” or what the intent of requirement is. Additionally, when the phrasing is used that includes that language “SCI with ERC hosting High and Medium Impact BCS or their associated PACS, EACMS, or PCA,” is the intent that only the BCS must be hosted on the SCI and the associated systems do not need to be hosted on SCI? An example of this language can be found in CIP-007 R4.1.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
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	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	
Document Name	
Comment	
Need clarification on CIP-005 R1.2.1 - Why restrict management systems to only share CPU with other Management Systems? Would it not be better to say BCS can only share CPU with other BCS? Can CPU be shared across Management Systems for BCAs and Management Systems for Non-BES Cyber Assets? Would you be able to clarify virtual CPU vs. physical CPU separation?	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
LCRA views many of these revisions as administrative in nature. They will require additional resources to update and reformat a NERC CIP Program. The result is a change to how programs are documented but not to security. Additionally, the rapid revisions of CIP Standards result in entities having to continually tweak their internal processes for collecting evidence and to ensure consistency with new terminology. Again, this is a concern if security is not being enhanced.	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	
Document Name	
Comment	

AEP appreciates the work of the SDT in addressing potential gaps related to virtualization in the currently enforceable language of the CIP Standards. It has been AEP's experience that there is adequate flexibility in the application of the current CIP Standards/requirements to allow for the implementation of Virtualization both as BES Cyber Assets/Systems, as well as the associated EACMS, PACS and/or PCA. This experience is based in Regional Entity(ies) audit of the virtualized environments that are currently operating in production CIP environments. We would further point out that the security and auditability of these systems, within the framework of the existing Standards, is supported by the CMEP Practice Guides released by NERC on 3/1/2021 (on the subjects of Virtual Network, Virtual Storage, and Virtual Systems).

Given prior successful audit of virtualized Assets within AEP's CIP environments, AEP recommends to consider limiting the introduction of new terms/definition to only those areas where it is necessary to reach an end result of increased security, resiliency and/or sustainability. AEP does, however, commend the movement away from heavily burdensome time-based requirements in favor of security-driven and objective-based requirements.

Please Note: one of AEP's balloters accidentally selected "Negative Opinion" for the CIP-002-7 Non-binding Poll. The intent was to select "No Opinion". While unable to change a vote once cast, AEP felt it was important to inform the SDT of the true intent of the vote.

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	
Document Name	
Comment	

LCRA views many of these revisions as administrative in nature. They will require additional resources to update and reformat a NERC CIP Program. The result is a change to how programs are documented but not to security.

Additionally, the rapid revisions of CIP Standards result in entities having to continually tweak their internal processes for collecting evidence and to ensure consistency with new terminology. Again, this is a concern if security is not being enhanced.

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 and would like to thank the SDT for allowing us to comment on the proposed changes.	
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	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	
Comment	
We continue to encourage the Standard Drafting Team to maintain full backward compatibility.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	
Comment	

CIP-006, R2 added “except during CIP Exceptional Circumstances” to the root requirement, but removed it from part 2.1. Are we to assume that the root requirement allowing CIP Exceptional Circumstances would flow down to the sub-parts? If so, why was If not removed from 2.2? If not, does this mean that first responders would be required to escorted? Clarity to the intent of the applicablility of this phrase would be appreciated.

The definition of IRA still leaves some room for interpretation. While DOminion Energy supports simpolifying the definition, the IRA definition should address the communication session that ends with the destination asset. The session between the asset (physical or virtual Cyber Asset) and the Intermediate System is user initiated. The session between the Intermediate System and the destination asset is user initiated.

A management console, for this example, does not have constant communication sessions with client Cyber Assets/Virtual Cyber Assets unless the console needs to execute a command on a client. A user establishes a session with the console, via multi-factor authentication, and instructs the console to execute a command on a client. In order to execute the command, the console needs to establish a communication session with the client.

Is a connection from console to a Cyber Asset client also a user-initiated IRA if the user schedules on the console a configuration command that will execute one hour later by the console (and after the user had ended the communication session to the console)? What if the user schedules a command for execution by the console within 5 minutes? Is this user-initiated IRA too? Would the console itself be an Intermediate System? The current language is ambiguos on these issues.

In both scenarios, the console establishes the communication sessions to the client asset and the sessions are not between the user and the client. Rather than leave the interpretation to the Entities or Regional Entities, the IRA definition should have more clarity built-in to address such scenarios.

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	
Document Name	
Comment	

Generic Formatting Comments

Issue 1:

The “Management Module” inclusion across the Standards is inconsistent with the inclusion of “Shared Cyber Infrastructure.” Tacoma Power believes there are additional locations where the risk posed by Management Modules is equivalent to the risk posed by the SCI itself and these should also include Management Modules as applicable. Tacoma Power suggests that there may be a way within the Applicability Section of the Standard to state that where SCI is included in the applicability of a requirement, any associated Management Modules are also included. This would avoid the issue of including one cyber asset within another, and the hall of mirrors that builds, which would happen if the SDT were to simply ensure Management Modules were included in the SCI definition. It would also simplify the Applicability Columns throughout. Another possible solution would be notating

each SCI applicability inclusion with a footnote, then including the statement that each inclusion of SCI also includes any associated Management Modules, as a footnote on each applicable page.

Issue 2:

Review each Standard's Applicability column to ensure the sub-bullet formatting and order of the "associated" PACS, EACMS, and PCA is consistent from unaltered to newly inserted items and across all Standards.

Issue 3:

The SDT should consider stating "per system or component capability" in the Requirement language instead of "per system capability". Requirements are applied at either the system or component level. Because there is inconsistency with the "level" of a Requirement's object across the CIP Standards, this change may add some necessary clarity.

CIP-005 General Comments

Issue 1:

Tacoma Power seeks clarification from the SDT on the directional language used in CIP-005. For example, the Standard uses "to and from", "leaving and entering", and "between". This inconsistency could be confusing depending on the context, consistency of usage could add clarity throughout the Standard.

Issue 2:

Comment on CIP-005 Technical Rationale, "Shared infrastructure and 'Mixed Trust' Risks": While Tacoma Power is not voting against this rationale document, we feel that affinity is not an adequate control to ensure SCI security in a mixed trust environment, because affinity controls exist on individual servers to split processor core access or RAM NUMA Node access.

In line with the above statement, perhaps changing the terminology used in describing the Affinity rule requirements (CIP-005 R1 Part 1.2, and CIP-005 R2 Part 2.6) to "Host or Cluster Affinity and Anti-Affinity rules" would provide more clarity to industry. Host Affinity is a VMWare Term, while Cluster Affinity is a Hyper-V term.

CIP-007 General Comments

Issue 1:

CIP-007 R1 Part 1.2 applicability column "Management Modules" entry includes PACS and EACMS where the rest of the Applicability entries do not, is this intentional? This appears to be a mistake.

Issue 2:

In CIP-007 R5 Part 5.7, the SCI entry in the Applicable Systems column includes "with ERC" which should be removed, as follows: "SCI at Control Centers hosting High Impact BCS, Medium Impact BCS or their associated:" Alternatively, Tacoma Power recommends the SDT re-word this applicability to state: "SCI hosting High Impact or Medium Impact at Control Centers or their associated:"

Issue 3:

While it may not be part of the SAR scope for Project 2016-02, Tacoma Power recommends that the SDT consider removing "at Control Centers" from the Applicability Statements from CIP-007 R5 Part 5.7 to enforce this control on those remote elements that are typically more exposed to attack.

CIP-010 General Comments

Issue 1:

The CIP-010 R2 Applicable Systems column omits SCI and Management Modules. Tacoma Power would like feedback from the SDT on whether this exclusion was intentional.

Issue 2:

Tacoma Power recommends that the SDT review and revise CIP-010, Attachment 1 to include SCI. There are instances of “BES Cyber System” which do not have the typical SCI redlined in.

Consistency with Project 2017-07

Project 2017-07 stated that “CIP-002-5.1a, CIP-003-6, CIP-003-7, CIP-004-6, CIP-005-5, CIP-005-6, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, and CIP-011-2 will not be revised at this time due to the current Project 2016-02 (Modifications to CIP Standards) and the CIP Standards Efficiency Review.” The currently posted redlines for Project 2016-02 do not include all of the Standards Alignment changes (e.g. “UFLS-only DP”). Tacoma Power recommends the SDT document whether this project or the CIP Standards Efficiency Review will closeout these updates.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

Ameren agrees with and supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	
Document Name	

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Please see comments submitted by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	
Document Name	

Comment

Too much compartmentalization based on non-industry standard definition. Please review NIST Publication 800-125 (virtualization guidelines) and apply controls, based on Terms such as Management Systems, Guest, Hosts, Network virtualization, Infrastructure virtualization (Mixed Trust, Resources sharing, high-watermarking) and similar guidance that is used by Industry, SME and vendors. SDT approach is complicated and confusing which will result in different interpretation by SMEs and ERO.

SDT draft utilizes non-industry standards requirements and terminology, and will result in confusion and subjective and varying application. Recommend that SDT use Industry standard terminology such as NIST or PCI-DSS and security controls as laid out in such frameworks.

All definitions should be contextualized in relation to BES application.

Furthermore, require standard requirements to apply control application based on risk to the systems based industry standard approaches such as high watermarking practices instead of compartmentalizing security controls based on every unique device types that SDT has identified.

SDT has summarily discarded Industry standard practices such as baselining but replaces it with subjective terms such as hardening, which varies depending on environment and device types. Such scenario will lead to different conclusions by the auditors and entity SME.

It has taken four years for the industry to standardize the security and baselining requirement. New approach discards all the work done so far and creates confusing set of expectations.

Further, in CIP-010, tracking hardening requirements in change management tickets is an incorrect approach as CM is for tracking activities and not performing assessments and compare of configurations.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	
Document Name	

Comment

Request clarification on CIP-005 R1.4 “per system capability.” Who determines that capability? What evidence do the auditors expect?

Request clarification on CIP-005 R2.3 “Multi-Factor Authentication (MFA).” Years ago, two step verification (2SV) was generally accepted as MFA. 2SV uses SMS which is hackable. Does this MFA expectation include 2SV?

Request consistency between CIP-005 R2.4 and R2.5. R2.5 Requirement uses abbreviation (IRA). R2.4 does not.

Several comments on CIP-005 R2.6; 1) the Applicable System should be explicitly stated; 2) we are concerned with how complex (difficult) Applicable Systems and Definitions are to comprehend; 3) is an Intermediate System *only* an Intermediate System; 4) does R2.6.2 allow communications with a remote system? 5) if Intermediate System is used only in R2, it should not be a defined term. The explanation and use of Intermediate System should be in only R2

Three comments on CIP-010 R3.2. These comments were repeated for CIP-010 R1.3. 1) request removal of “minimizes differences with the production environment” because new language is a) subjective, b) better suited to the measures and c) the previous language is sufficient 2) if this language cannot be removed, request clarification that the entity determines “minimal differences” 3) suggest that the intent is to a) test and b) document what was tested

For CIP-010 R3, request that the SCI requirement into a separate Part. Same comment was made for CIP-010 R1

One comment on CIP-007 R1.3. Request consistent language on the exclusion of services that cannot be disabled. Consistent with R1.1.

One comment on CIP-007 R2. Concerned about this language. The proposed language is “systems.” However, patches are applied to assets. This concern is repeated in CIP-007 R4.1, R4.2, R4.3, R5.4, R5.5, R5.6

One comment on CIP-007 R3.1 Measures. This is a repeat of a general comment on CIP-007. The use of “system hardening” here seems different than “system hardening” elsewhere in CIP-007. Request consistent use of this label. How does one measure “system hardening.” What evidence will the auditors expect?

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/comments submitted by EEI

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

This is a significant change and overhaul of all the CIP Standards and Requirements that will require a significant re-analysis of stable and current CIP Standards and Requirements and definitions. Today, virtualization is used with the understanding that the VM host receives the “high water mark” of the VMs hosted, which is a simplified approach that doesn’t require new definitions. Texas RE cautions the splitting of compliance and security controls to components of VM host(s) in virtualization.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

N/A.

Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	
Document Name	
Comment	
Wabash Valley appreciates the effort that the Standards Development Team has put into development of this standard. However, significant additional work and documented guidance such as those that would previously have been found in the Guidelines and Technical Basis Section of the CIP Standards is needed and should be a mandatory consideration of CMEP teams. The removal of these sections has been a detriment to the CIP Reliability 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	
Document Name	
Comment	
We would like to thank the SDT for their hard work and would like to thank the SDT for allowing us to comment on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	
Document Name	
Comment	
N/A	

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

no further, thank you.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	
Document Name	

Comment

For CIP-006 R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	
Document Name	

Comment

SPP wants to the thank the SDT for their work on this complex project and understands the time and effort that goes into an undertaking such as this.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

PG&E has no further comments related to this Command & Ballot.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	
Document Name	

Comment

Management Systems for non-virtual environments should be protected at the same level as the Management Systems for SCI; we understand that the SAR limited the SDT. Likely this could be captured by FERC as a conditional approval item for the next version of CIP Standards.

Please keep ESP and EAP as NERC Glossary terms. This may avoid future auditor interpretation issues and allow consistent application of the concepts across industry. It also helps preserve backward compatibility.

Please provide a draft copy of the NERC CIP ERT for the new requirements with the next posting. This would help entities assess the impacts the proposed changes would have to managing audit preparationunder the new requirements.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for details.

Likes 0	
Dislikes 0	

Response

Jose Avendano Mora - Edison International - Southern California Edison Company - 1,3,5,6

Answer	

Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
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 signs on to the comments provided by the SRC and submits the following additional comments: 1) PJM requests additional clarity surrounding the removal of the term “or” in CIP-007 R2.3. Does this change the context of the standard or was the second “or” kept intentionally to provide choice in the list of actions? Recommendation: remove the second “or” for consistency. 2) PJM identifies that the CIP 011 requirements are being modified to focus on the BCSI itself and not the actual Cyber Assets identified in the “Applicable Systems” column. PJM recommends that the applicable systems column should include "BCSI repositories" rather than the Cyber Assets identified in the “Applicable Systems” column, given that the requirements are being modified to focus on the BCSI itself and not the Cyber Assets. 3) PJM also requests SDT to confirm intention of listing SCI with EACMS, PACS, and PCA in the applicable system sections which seems repetitive. The new definitions for EACMS, PACs, and PCAs now includes SCI which makes the Applicable Systems section repetitive when listing “SCI hosting High or medium impact BCS or their associated EACMS, PACS, and PCA”.	
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	
Request clarification on CIP-005 R1.4 “per system capability.” Who determines that capability? What evidence do the auditors expect?	

Request clarification on CIP-005 R1.5. The proposed language does not include the combination of non-IP and malicious. Is this acceptable?

Request clarification on CIP-005 R2.3 “Multi-Factor Authentication (MFA).” Years ago, two-step verification (2SV) was generally accepted as MFA. 2SV uses SMS which is hackable. Does this MFA expectation include 2SV?

Suggest a CIP Standard should not explicitly reference a Standard not in NERC’s purview in Requirement language. If the inclusion is necessary, request correction of CIP-005 R2.4’s references to GOOSE protocol - “IEC TR-61850-90-5 R_GOOSE.” We believe SDT should reference 1) IEC/TR 61850-90-5:2012 / Part 90-5: Use of IEC 61850 to transmit Synchrophasor information according to IEEE C37.118 and 2) IEC 61850-8-1 GOOSE (Generic Object-Oriented Substation Event message) and IEC 61850-9-2 SV packets. CIP-003 may have shared this concern.

Request consistency between CIP-005 R2.4 and R2.5. R2.5 Requirement uses abbreviation (IRA). R2.4 does not.

Several comments on CIP-005 R2.6; 1) the Applicable System should be explicitly stated; 2) we are concerned with how complex (difficult) Applicable Systems and Definitions are to comprehend; 3) is an Intermediate System *only* an Intermediate System; 4) does R2.6.2 allow communications with a remote system? 5) if Intermediate System is used only in R2, should not be a defined term. The explanation and use of the Intermediate System should be in only R2

Two comments on CIP-005 R3. 1) system to system communications is not currently defined. Is system to system included in R3? The issue is that that “system to system” is nebulous; 2) request an illustration/diagram since this is hard to follow

Three comments on CIP-010 R3.2. These comments were repeated for CIP-010 R1.3. 1) request removal of “minimizes differences with the production environment” because new language is a) subjective, b) better suited to the measures and c) the previous language is sufficient 2) if this language cannot be removed, request clarification that the entity determines “minimal differences” 3) suggest that the intent is to a) test and b) document what was tested

For CIP-010 R3, request that the SCI requirement into a separate Part. The same comment was made for CIP-010 R1

One comment on CIP-007 R1.3. Request “consistent” language on the exclusion of services that cannot be disabled. Consistent with R1.1.

One comment on CIP-007 R2. Concerned about this language. The proposed language is “systems.” However, patches are applied to assets. This concern is repeated in CIP-007 R4.1, R4.2, R4.3, R5.4, R5.5, R5.6

One comment on CIP-007 R3.1 Measures. This is a repeat of a general comment on CIP-007. The use of “system hardening” here seems different than “system hardening” elsewhere in CIP-007. Request consistent use of this label. How does one measure “system hardening?” What evidence will the auditors expect?

Suggest not to include PACS and EACMS into the scope in the context of SCI as this requirement doesn’t exist for a PACS and EACMS, not on an SCI. SAR is for including the virilization concepts not to add additional controls.

Suggest reviewing the Applicable Systems of the different CIP associated with management modules. The current language only refers to Management Modules of SCI hosting what about the management module of a BCA? Management Modules of SCI hosting would have more controls than Management Modules of BCA.

SDT should look into the CMEP Practice Guides publish on the NERC website. The following documents; CMEP Practice Guide Virtual Systems, CMEP Practice Guide Virtual Network, CMEP Practice Guide Virtual Storage is pertaining to virtualization and they contain enough elements for us to understand what needs to be done to be compliant. Those CMEP documents permit the usage of virtualization with the current concepts and definitions. SDT should use those documents and update the different CIPs documents with the required and corresponding wording.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb 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; - Douglas Webb

Answer	
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 19,

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Every CIP Reliability Standard currently in effect makes every Distribution Provider that owns underfrequency (UFLS) systems that meets the subparts identified in 4.1.2.1.1 and 4.1.2.1.2 applicable to the CIP Standards, however, UFLS only Distribution Providers that may also meet these criteria are not currently applicable to any of these standards. EEI requests that this gap be addressed by adding UFLS only Distribution Provides that meet the identified criteria to be made applicable to these Reliability Standards.

EEI seeks clarification CIP-005 R1.2.1 to understand the reason for restricting management systems to only share CPU with other Management Systems. We recommend the language be revised to state that BCS can only share CPU with other BCS. Additionally, should CPU be shared across Management Systems for BCAs and Management Systems for Non-BES Cyber Assets?

EEI request clarification on whether segmentation can be achieved through policies or does segmentation need to occur on separate physical blades (air gap)?

CIP-005, Requirement R2, Part 2.2: states, “Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.” EEI understands this to mean that encryption is only required between user/client and the IS and not between the IS and the BCS. In the substation remote access case the Intermediate System may be at a central location (Control Center/Data Center) and the link to the BCS may travel many miles over links owned by providers (i.e., telecom carriers). This appears to imply that not encrypting this communication is acceptable. This appears to be a gap that should be addressed or clarified.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	
Document Name	

Comment

CPS Energy recommends revisions that do not drastically change the existing standards. Backwards compatibility is not evident in the revisions. Additonally, the attention given to virtualization feels over weighted compared to non-virtualized systems and may increase burden to entities.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	
Document Name	

Comment

With the revisions to CIP-005 R1.5 and move to allow a zero trust model it is unclear in the revision what measure would meet this for a single device with its own logical isolation. The host may not have an IDS or application layer firewall. Would a host with AVAM used for CIP-007 R3 be sufficient to met this requirement?

We have a concern about CIP-010 R2.1. The monitoring would now expand in scope to R1.1.6 items. Items R1.1.1 through R1.1.5 are properties of a device and R1.1.6 is security settings applied to a device. One of these things are not like the others. So why does the monitoring have to include only the security settings in R1.1.6 but not the other CIP-005 or CIP-007 securty controls? We recommend striking R1.1.6 from being in scope for CIP-010 R2.1.

While the Implementation does allow for early adoption it is unclear if the requirements must be adopted all at once or if an entity can adopt part of the standards and have a staggered implementation. If such a staggered implementation is allowed then is there an order that some must be adopted first as others are dependent on the first?

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	
Document Name	

Comment
Request putting ‘Baseline configuration in the Standard somewhere to make the CIP-010 backwards compatible.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1	
Answer	
Document Name	

Comment
Please see JEA coments, an individual response to my comment is not required.

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 that as drafted, CIP-005-8 Requirements R2 and R3 are contradictory. Specifically: R2 Part 2.1, which mandates the use of an Intermediate System for IRA, applies to SCI with IRA hosting High or Medium Impact BCS or their associated, PCA, PACS, or EACMS. At the same time: R3, originally developed for vendor remote access to EACMS and PACS, and which does NOT mandate the use of an Intermediate System, applies to SCI hosting EACMS or PACS associated with High or Medium impact BCS. As written, both R2 and R3 would seem to apply to an SCI hosting, for example, EACMS associated with High Impact BCS. N&ST also believes allowing “no IS” vendor remote access to SCI that happen to be hosting only EACMS and/or PACS (and their associated Management Modules) creates an unacceptable security risk. We believe that all vendor remote connections to ANY SCI should require the use of an Intermediate System if there’s a person typing on a keyboard at the vendor location. We believe, further, that this position is consistent with the SDT’s stated goal of addressing security risks associated with serial IRA.

N&ST believes these issues can be simply resolved by making the following changes:

For R2 Parts 2.1, 2.4, and 2.5, revise “Applicability” so those parts apply to SCI hosting High or Medium Impact BCS or their associated PCA, PACS, or EACMS. Make the same applicability changes for Management Modules.

For R3, delete ALL proposed changes. N&ST believes CIP-005-7 R3 already covers both virtual and physical EACMS and PACS as written.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Although the acronyms for BCS, SCI, and BCSI are addressed at the beginning of the standards, ERCOT suggests all terms should be spelled out at the beginning of applicable requirement language because the requirement language is the most used and referenced part of a reliability standard. This will aid in readability.

ERCOT appreciates the work to address virtualization. However, based on the differences in technology between legacy system and virtualized systems, the SDT should consider moving the virtualization requirements into a separate standard that addresses only the requirements applicable to virtualized environments. The SDT has received comments over time regarding the confusion that will be created by intermingling the legacy requirements and virtualization. If an entity has no intention of using virtualized systems, they may be confused by which requirements they should follow and how they would apply.

In the purpose of CIP-013, “and their associated cyber systems” was added. Using “cyber systems” may lead to confusion and inconsistent applicability by using undefined terms.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

- **CIP-005, Requirement 1, Part 1.3** – the SDT proposes to eliminate the requirement to “Require inbound and outbound access permissions…and deny all other access by default.” This, coupled with the elimination of the ESP and EAP concepts, increases the complexity of demonstrating where security starts and stops. What keeps the sprawl in check? Could the SDT describing their thinking on this in the Technical Rational document?

- **CIP-005, Requirement 1, Part 1.5** – the proposed changes are problematic because an entity “must detect” as opposed to “having a method to detect.” How can an entity know or demonstrate that they are able to detect *all* known or suspected malicious Internet Protocol communications?

Recommendation: SRC proposes the following lanuguage for Part 1.5: “**Have one or more method(s) for detecting** known or suspected malicious Internet Protocol (IP) communications…”

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	
Document Name	

Comment

In general, AWS supports the proposed requirements revisions to accommodate on-premises use of virtualization. Understanding that this SDT is focused on virtualization as it relates to on-premises, we read the revisions with the multiple uses of virtualization and emerging technologies in mind to consider language for both current and future applicability.

Comment #1

Virtualization technology provides powerful capabilities for logical separation. The Technical Rationale documentation makes clear that logical isolation methods are as effective as physical methods, including when used in mixed trust environments. The proposed requirements like those in CIP-005 R1 Part 1.2; CIP-005 R2 Part 2.6; and, CIP-010 R1 Part 1.1, do not differentiate or explicitly state that logical or physical isolation methods are acceptable, which we read as providing the Responsible Entities the flexibility to use either logical or physical isolation to meet the requirements. If this is the intent then a useful addition would be for the requirements to explicitly state this either with a universal, over-arching statement or within the requirement language.

Comment #2

The CIP-004 or CIP-011 requirements do not state that encryption of BCSI is sufficient in demonstrating prevention of unauthorized access of BCSI. It’s important that the requirements are clear on this point, therefore we recommend that they explicitly state that individuals obtaining encrypted BCSI without the ability to use it within a meaningful timeframe should be considered as not having access. This is in accordance with the CMEP Practice Guide BES Cyber System Information. We recognize that a separate drafting team is addressing BCSI. We raise it here to encourage coordination and avoid unnecessary revision in the future.

Thanks to the SDT for the hard work to revise the requirement language and support adoption of technology in a secure and compliant manner.

Likes 0	
Dislikes 0	

Response	
Wayne Guttormson - SaskPower - 1	
Answer	
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	

Comments received from Paul Shipps – Lakeland Electric

1. The SDT added, revised, and retired 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

Definitions changes are extremely confusing and do not follow Industry standard terminologies. Many terminologies do not reference BES and hence its extemly confusing.

Further, most new definitions are not required and just BCS definition is sufficient. All other elements must follow, high watermarking and security controls and standards must apply.

2. CIP-005 Requirement R1 part 1.1 was revised to permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

There is no need to change a pre-established definition such as ESP. New application creates extreme confusion for application of security for cyber assets. Compartmentalization should be based on security enclaving but high water marking. A VLAN should be high water marked to Cyber Asset level as BES function will be impacted if it is compromised.

It seems SDT has compartmentalized assets in order to limit compliance application. Selective application of controls will result in significant security risks.

3. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

System should continue to follow security model of complete distrust. Only communication that is required must be allowed. This can only be established if rules are explicit including, Source, destination, Ports and Protocol. New application is very subjective and confusing. Industry is currently using Goose and still compliant, why change configuration and standards must be technology neutral.

4. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.

- ○ Yes
- ◉ No

Applicability section is confusing. Too much compartmentalization of devices and non-industry standard definition are not needed. BCS definitions should be updated to address logical assets and apply high water marking.

Current approach limits security with assumption that associated devices can be compromised externally, but BES impact must be considered if Cyber system is compromised and made unavailable.

5. The SDT modified CIP-005 Requirement R2 to ensure remote access management requirements align with the new and revised virtualization terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ( ) Yes
- (•) No

"Ensure that authorized IRA is through an Intermediate System. " – Can we communicate through the firewall. Previous standard was accurate. New standard is subjective and will create confusion.

6. The SDT revised CIP-007 Requirement R1 Part 1.1 to shift the security objective from logical network accessible ports to services. The proposed revisions require Responsible Entities to enable only network accessible services that have been determined to be needed by the Responsible Entity. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ( ) Yes
- (•) No

Unnecessary confusion. Previous standard language was sufficient for design of security controls and application. Revert to old standard, which industry has worked hard to standardize and create controls that have been effective.

7. CIP-010 Requirement R1 currently requires Responsible Entities to develop a baseline configuration, authorize changes to the baseline, and document the changes. The SDT proposes to revise Requirement R1 to remove the reference to baseline configurations. The proposed revisions require the authorization of changes to Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible ports, security patches applied, and SCI configurations. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ( ) Yes
- (•) No

SDT has created an uncalled for scenario where, they have removed Baselines but left the baseline elements intact, this is causing significant confusion amongst SME.

Requiring CM as method of compliance will set a serious challenge and will limit ability to secure system as CMs do not include security baseline information, only the proposed changes, but assessment are never included in CM, just a summary of results.

This whole approach will result in inaccurate and subjective application and often result in contention with compliance and auditors.

Current CIP-010 standards and requirements are matured and industry has made significant process developing good controls. There is absolutely no reason to change as these changes do not improve security but are detrimental.

8. The SDT modified CIP-010 Requirement R3 Part 3.3 to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. The revised requirement allows the use of remediation VLANs to perform active vulnerability assessments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ( ) Yes
- (•) No

Too much compartmentalization based on non-industry standard definition. Please review NIST Publication 800-125 (virtualization guidelines) and apply controls, based on Terms such as Management Systems, Guest, Hosts, Network virtualization, Infrastructure virtualization (Mixed Trust, Resources sharing, high-watermarking) and similar guidance that is used by Industry, SME and vendors. SDT approach is complicated and confusing which will result in different interpretation by SMEs and ERO.

9. CIP-002-5.1a includes exemption 4.2.3.2, which exempted Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. In the development of conforming changes, the SDT determined that the exemption should be split into two distinct exemptions to adequately cover all cyber systems associated with conforming changes. The SDT established those conforming changes in proposed Exemptions 4.2.3.2 & 4.2.3.3. Do the changes clearly identify the exempted cyber systems? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

Many entities have virtualized systems and were compliant with CIP in recent audits. Please do not over complicate. Focus on security or where gaps exists. Only changes to BCS to include virtual environment and logical asset configuration is required.

10. BCS and SCI are mutually exclusive by definition, however SCI poses a significant reliability risk to the Bulk Electric System. The SDT considered the risks associated with SCI and revised CIP-002 Requirement R1 to include the identification of SCI in Parts 1.3, 1.4, and 1.5. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

BCSI requirements are sufficient as in CIP-004 and CIP-011. Entities are compliant and appropriate controls are available to secure BCSI in current version.

Shared storage housing active BCS data should not be allowed for mixed trust environments and introduces significant risk to BES.

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

11. In the current enforceable standards, there are no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement. The SDT revised CIP-002 to include the identification of SCI associated with EACMS, PACS, and PCAs to help address this issue within the virtualization scope of the current SAR. The proposed requirement could reduce possible non-compliance to a single issue if a Responsible Entity fails to properly identify SCI associated with EACMS, PACS, or PCAs. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

Based on comments above, these changes are confusion and are detrimental to security.

12. The SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved Request for Interpretation (RFI) regarding "shared BES Cyber Systems." The SDT modified the criterion to reference each discrete shared BCS. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

13. The SDT made conforming changes to CIP-003 and CIP-004. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

Current standards are sufficient and these changes are cosmetic. No changes to CIP-004 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

14. The SDT modified the Applicable Systems column in CIP-006 to include SCI hosting PACs associated with Medium Impact BCS with ERC or IRA. The SDT made the proposed revisions to clarify the scope of requirements that apply when an entity implements serial IRA. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ◉ Yes
- ○ No

15. The SDT made conforming changes to CIP-008 and CIP-009. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

Current standards are sufficient and these changes are cosmetic. No changes to CIP-008 or 009 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

16. The SDT modified CIP-011 Requirement R2 part 2.1, which will allow cryptographic erasure in scenarios where BCSI can't be mapped to particular disks in virtualized storage. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

Current standards are sufficient and these changes are cosmetic. No changes to CIP-007 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

Mixed trust environment should not be permitted for BCS.

BCSI requirements are sufficient as in CIP-004 and CIP-011. Entities are compliant and appropriate controls are available to secure BCSI in current version.

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

17. The SDT performed a review of the CIP Standards and determined that CIP Exceptional Circumstances could be applied to the following additional requirements: CIP-004-7 Requirement R2 Part 2.2, CIP-004-7 Requirement R3 Part 3.5, CIP-006-7 Requirement R1 Part 1.8, CIP-006-7 Requirement R1 Part 1.9, CIP-006-7 Requirement R2, CIP-010-5 Requirement Part 1.2, and CIP-010-5 Requirement R1 Part 1.3. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- ○ Yes
- ◉ No

Current standards are sufficient and these changes are cosmetic. No changes to CIP-007 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition

18. Implementation Plan: The SDT proposes an Implementation Plan that makes the revised CIP Standards and definitions effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order. However, the implementation plan allows a Responsible Entity to elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. Do you agree with this proposal? If you think an alternate effective date is needed, please provide a detailed explanation of actions and time needed.

- ◉ Yes
- ○ No

19. Please provide any additional comments for the SDT to consider, if desired.

Too much compartmentalization based on non-industry standard definition. Please review NIST Publication 800-125 (virtualization guidelines) and apply controls, based on Terms such as Management Systems, Guest, Hosts, Network virtualization, Infrastructure virtualization (Mixed Trust, Resources sharing, high-watermarking) and similar guidance that is used by Industry, SME and vendors. SDT approach is complicated and confusing which will result in different interpretation by SMEs and ERO.

1. SDT draft utilizes non-industry standards requirements and terminology and, will result in confusion and subjective and varying application. Recommend that SDT use Industry standard terminology such as NIST or PCI-DSS and security controls as laid out in such frameworks.

2. All definitions be contextualized in relation to BES application.

3. Furthermore, require standard requirements to apply control application based on risk to the systems based industry standard approaches such as high watermarking practices instead of compartmentalizing security controls based on every unique device types that SDT has identified.

4. SDT has summarily discarded Industry standard practices such as baselining but replaces with subjective terms such as hardening, which varies depending on environment and device types. Such a scenario will lead to different conclusions by the auditors and entity SME.

5. It has taken four years for the industry to standardize the security and baselining requirement. New approach discards all the work done so far and creates confusing set of expectations.

6. Further, In CIP-10, tracking hardening requirements in a change management tickets is incorrect approach as CM are for tracking activities and not performing assessments and compare of configurations.