NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2016-02 Modifications to CIP Standards | Virtualization - Draft 4
Comment Period Start Date:	8/17/2022
Comment Period End Date:	10/7/2022
Associated Ballot(s):	2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 AB 4 ST

There were 72 sets of responses, including comments from approximately 188 different people from approximately 121 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Director, Standards Development Latrice Harkness (via email) or at (404) 858-8088..

Questions

1. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

2. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

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

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

5. The SDT has used phrasing such as "SCI supporting an Applicable System from this Part" in the Applicable Systems column across many of the standards. Is it clear that this scopes the requirements for SCI to match the system(s) it hosts?

6. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

7. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes or scoping clarifications related to SCI. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

8. The SDT has revised the Implementation Plan to include 3 defined early adoption dates as options should Responsible Entities choose to do so. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

9. Please provide any additional comments for the standard drafting team to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
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
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Boeshaar	WEC Energy Group, Inc.	6	RF
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
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	3,5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jamie Monette	Allete - Minnesota Power, Inc.	1	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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					George Brown	Acciona Energy North America	5	MRO
					Jaimin Patel	Saskatchewan Power Corporation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	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
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Public Utility District No. 1	Meaghan Connell	5		PUD No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1	3	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
of Chelan County						of Chelan County		
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
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
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Dana Showalter	Electric Reliability	2	Texas RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
				(SRC) 2016-02 Virtualization (Draft 4)		Council of Texas, Inc.		
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	IS-NE	2	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SERC
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	5	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Company Services, Inc. - Gen		
DTE Energy	patricia ireland	4		DTE Energy	Patricia Ireland	DTE Energy - Detroit Edison	4	RF
					Karie Barczak	DTE Energy - Detroit Edison Company	3	RF
					Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Gerry Dunbar	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
					Harish Vijay Kumar	IESO	2	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	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
Tim Kelley	Tim Kelley		WECC	SMUD / BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					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	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Cooperative, Inc.		
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST sees no reason to change the existing definition's use of "remote access client or other remote access technology." The second part of the proposed definition would, as written, apply to any remote connection using a communications path that included routable to serial conversion, regardless of where that conversion took place (e.g., remote location vs. "local," or "inside the BES asset" location). NST is aware of concerns that using phrases such as "outside the asset" in this context might cause confusion about its relationship to electronic access control requirements for BES assets containing low impact BCS, but we nonetheless recommend using it to avoid overly broad application of "IRA" to communications using both routable and serial wide-area connections.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT asserts that the scenario must meet the definition of IRA in order to be in scope of the requirement. The current definition is not clear as to whether a device that is serial only, and thus has no "associated ESP", can have IRA at all. The SDT is making this scenario clear in scope of the definition, so that the requirements in CIP-005 R2 are applied. The SDT also removed phrases such as "outside the asset" and "remote access client or other remote access technology." in response to previous comments concerning what those terms mean, especially now with the use of SSL VPNs and other methods that require no client "remote access" software.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	

The term “Cyber System” is too broad in scoping IRA. Suggest revise to clarify that the target of IRA is BES Cyber System rather than “Cyber System” to avoid including EACMS, SCI, PCA, etc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Definitions and scoping are separate, therefore, do not scope requirements. The SDT, by defining the glossary term IRA, is describing a type of access. Similarly, in defining Cyber System, the SDT is describing a collection of Applicable System types that are collectively referred to as the defined term. The Glossary of Terms is the dictionary for what each term means. The scoping of CIP requirements is achieved through requirement language where the term is used, in combination with the Applicable Systems column for each corresponding Requirement Part.	
Tim Kelley - Tim Kelley 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; - Tim Kelley, Group Name SMUD / BANC	
Answer	No
Document Name	
Comment	
Under the new definition of IRA, bullet 5 that excludes “Communication that originates from an Intermediate System; or,” should not be excluded from the definition. Excluding it would be confusing as IRA to a BCS should come from an Intermediate System. The new definition of IRA conflicts with the existing definition of ERC. ERC is the ability to access a BCS through its ESP via a “bi-directional” routable protocol connection. In the new IRA definition, the second bullet addressing serial Cyber Assets states that IRA is “User-initiated electronic access by a person using a routable protocol” (*not necessarily bi-directional*), “that is converted by the Responsible Entity to a non-routable protocol….,” is in direct conflict with the existing definition of ERC. This is not a concern over serial end points being in scope or not, we all agree that they are in scope, but the term “bi-directional” does nothing to help bring serial devices into scope, in fact it implies that serial devices that do not establish TCP/IP connections are out of scope. Our recommendation to the SDT is to modify the definition of ERC as follows. First, remove the words “bi-directional” since there is no such thing as bi-directional routable protocol. Changing the ERC definition to simply “routable protocol” would create consistency throughout the	

requirements. Second, remove the word “connection” as this term implies that there has been a TCP handshake and a connection is established while excluding connectionless protocols such as UDP. Consider using “routable protocol communication” or just “routable protocol”. In CIP-005 R1.2, reference is made to routable protocol communication instead of connection, so the SDT may want to align with that if they are using the term routable protocol is not enough.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees “Communication that originates from an Intermediate System; or,” should not be excluded from the IRA definition and has removed that phrasing. The SDT decided to retain the proposed language in the ERC definition. The SDT asserts IRA describes a particular access type, whereas ERC describes a transport mechanism for which the access type of IRA is accomplished. The ERC definition is used as a scoping mechanism within the Applicable Systems of Requirement Parts, whereas IRA itself is an access type for which particular controls defined in CIP-005 R2 must be implemented. The SDT addressed the concern about directionality of the routable protocol connection within the IRA definition by clarifying IRA, including "...using a routable protocol • That is converted by the Responsible Entity to non-routable protocol "that allows access" to a Cyber System;...".	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
Should “or” be added to the end of the first bullet to more clearly define the need to continue dropping through the bullets like a decision tree to identify if any of the points are true instead of exiting after the first question? It is unclear if after the first bullet is an “and” or an “or” to identify IRA.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Reference the word version of the Results-based Standard template (link) on the NERC Resource page. Numbered lists indicate an “and” and bulleted lists indicate an “or.” The location of the “or” means that each bullet would read with an “or” as you move to the next bullet.	

Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Changes to the IRA definition adds conversion from routable to non-routable (serial) communications to remote BCS that was previously omitted. Further clarifications in the definition of IRA removes some gray areas and further delineates IRA from system-to-system communications. However, there remains 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 enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to the definition to ensure validity of communications to Applicable Systems regardless of source or intent. In addition, approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization and approval of SCI terminology and other definitions associated with virtualization. The SDT has added rationale but not defined whether user-created scripts and programs that can be modified and scheduled to run independently are considered IRA – even though an unauthorized user could modify it to their benefit. Both scripts and programs can be user-initiated, and with no definition of system-to-system communications there are still lingering issues regarding what system-to-system communications is comprised. Further, user-created scripts and programs may not be capable of reading multi-factor tokens or their displayed codes, but additional security for these connections can be implemented through certificates and the use of secure connections via SSH or SSL.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT maintains there is a long standing issue where "system to system" communications (covered by CIP-005 R1) could need and use protocols/ports that can also be used for IRA. The SDT asserts that IRA is focused on the human interaction with the Applicable System and the associated capability for a human to access and remotely interact with an Appliable System. Not the interactive capability of a given protocol/port that may also be needed for process-based system-to-system communication, relying on other CIP-005 and CIP-007 requirements to restrict communications and secure the Applicable System. If a protocol is used for IRA, then CIP-005 R2 controls must be applied to that access. However, the R2 controls are designed for interactive users only; Applying those controls to non-user interactive sessions (system-to-system) would break automated system-to-system data transfers and the like that may be needed for reliable operation of the BCS. Therefore, the SDT cannot apply R2 controls in a mandatory manner to these protocols/ports that have multiple uses, such as secure batch file transfers between processes and interactive user logon. The SDT is concerned with how a mandatory requirement preventing IRA (or considering system-to-system communication using certain IRA capable protocols/ports) in these specific situations could be constructed, as in some cases entities may use the protocol/port to	

perform both, while also having the proper controls on both. The SDT has not defined scripts and programs scheduled to run independently as IRA for the reasons noted - the R2 controls would break such functionality.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
The revised definition of IRA provides more clarity than the earlier version. With that said, AEP recommends removing second bullet under what “IRA does not include” list, as IRA should include “communication that originates from an Intermediate System”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees and made the corresponding change in the definition as well as in requirements to avoid the "hall of mirrors" effect regarding recursive Intermediate Systems, which the bullet was originally intended to prevent.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. It is up to each Registered Entity to determine which serial connections meet the updated IRA definition and proposed requirement language, and an entity would need to know what Applicable Systems a user can initiate remote access (IRA) to even if the device is serial only. For example, a serial cable from a terminal server connected to the console port of an Applicable System that can be accessed remotely benefits	

from re-evaluation to see if it meets the new definition of IRA and would need CIP-005 R2 controls on the routable protocol part of the overall path. Thus, this is not an evaluation of all serial, but an evaluation where a user can remotely access on the serial side of IP-serial converters/terminal servers only.	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No
Document Name	
Comment	
Suggest change to ¨To a Management Interface of Shared Cyber Infrastructure protected by an ESP¨. As management interface of target SCI should be located inside ESP and SCI outside ESP should not be in scope. Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. It is up to each Registered Entity to determine which serial connections meet the updated IRA definition and proposed requirement language, and an entity would need to know what Applicable Systems a user can initiate remote access (IRA) to even if the device is serial only. For example, a serial cable from a terminal server connected to the console port of an Applicable System that can be accessed remotely benefits from re-evaluation to see if it meets the new definition of IRA and would need CIP-005 R2 controls on the routable protocol part of the overall path. Thus, this is not an evaluation of all serial, but an evaluation where a user can remotely access on the serial side of IP-serial converters/terminal servers only.	
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 confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. It is up to each Registered Entity to determine which serial connections meet the updated IRA definition and proposed requirement language, and an entity would need to know what Applicable Systems a user can initiate remote access (IRA) to even if the device is serial only. For example, a serial cable from a terminal server connected to the console port of an Applicable System that can be accessed remotely benefits from re-evaluation to see if it meets the new definition of IRA and would need CIP-005 R2 controls on the routable protocol part of the overall path. Thus, this is not an evaluation of all serial, but an evaluation where a user can remotely access on the serial side of IP-serial converters/terminal servers only.	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	
The IRA definition contains “To a Manangement Interface of Shared Cyber Infrastructure”. We feel this should read “To a Management Interface”. Adding SCI to the definition restricts the scope to just Management Interfaces on SCI. Management Interface’s definition contains SCI, so it is unnecessary to put SCI into the requirement as well.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees and changed the definition to "To a Management Interface" and moved all scoping to the standard within the Applicable Systems and Requirement Parts. CIP-005 R1.3 was rewritten to incorporate the security objective of protection of the configuration of ESPs and SCI, leaving the method to the entity.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	

We suggest that IRA definition should remain unchanged and have the specific scenarios that these definition changes are attempting to address become part of the standard requirement language. (i.e. CIP-005-8 R2).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT asserts that the scenario must meet the definition of IRA in order to be in scope of the requirement. The current definition is not clear as to whether a device that is serial only, and thus has no "associated ESP", can have IRA at all. The SDT made this scenario clear in scope of the definition, so that the requirements in CIP-005 R2 are applied.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Request confirmation that entities should re-evaluate serial connections because they may now be in scope due to the updated definitions of IRA and ERC.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. It is up to each Registered Entity to determine which serial connections meet the updated IRA definition and proposed requirement language, and an entity would need to know what Applicable Systems a user can initiate remote access (IRA) to, even if the device is serial only. For example, a serial cable from a terminal server connected to the console port of an Applicable System that can be accessed remotely benefits from re-evaluation to see if it meets the new definition of IRA and would need CIP-005 R2 controls on the routable protocol part of the overall path. Thus, this is not an evaluation of all serial, but an evaluation where a user can remotely access on the serial side of IP-serial converters/terminal servers only.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	No
Document Name	

Comment	
The SRC suggests that IRA definition should remain unchanged and have the specific scenarios that these definition changes are attempting to address become part of the standard requirement language. (i.e. CIP-005-8 R2). 1. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT asserts that the scenario must meet the definition of IRA in order to be in scope of the requirement. The current definition is not clear as to whether a device that is serial only, and thus has no "associated ESP", can have IRA at all. The SDT made this scenario clear in scope of the definition, so that the requirements in CIP-005 R2 are applied.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the proposed changes for the IRA definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	

AZPS agrees with the IRA definition modifications.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
WECC suggests that the CIP-005-8 R2.4 use of 'vendor remote access' in the applicable system is not consistent with 'active vendor remote access sessions' and causes confusion considering neither term is defined. WECC suggests removing 'vendor remote access' from the applicable systems and have the scope of 'active vendor remote access sessions' stand on its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees and removed the phrase.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE agrees with the revisions to the IRA definition. Use of an Intermediate System to access systems that convert routeable to non-routable protocol adds a mandatory MFA step that may not be present in current implementations, and logs use of those systems.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) agrees with the revisions to the IRA definition. Use of an Intermediate System to access systems that convert routeable to non-routable protocol adds a mandatory MFA step that may not be present in current implementations, and logs use of those systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for the hard work in developing this definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the revised Interactive Remote Access (IRA) definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Chelan appreciates the SDT's work on IRA and CIP-005 and approves the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Thank you to the SDT for clarifying what is and what is not applicable.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the revised definition of IRA.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
MRO does not understand the need for the qualifier 'by the Responsible Entity' added to the conversion to non-routable. This seems like it would give entities a way out of compliance with the IRA requirements around serial communication by having someone else convert it.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT added the phrase in response to comments on previous drafts. For circuits that go between different entities, such as between a BA and a GO/GOP, the generator may only have a serial connection they connect to their system. They do not know whether the serial is converted to IP at any point along the path to the BA. To make this clear, the entity that does the conversion from IP to serial is the one that will need, if IRA is allowed over the path, to implement CIP-005 R2 controls on the IP side of the conversion. The generator cannot do that in this scenario. The SDT asserts that the entity that performs the conversion needs to be concerned, not the entity that simply has a serial cable to connect to. The TR was be modified to address the concern.	

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	
Donald Lock - Talen Generation, LLC - 5	
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	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 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	
Israel Perez - Salt River Project - 6	
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	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 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	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh

Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
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	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kinte Whitehead - Exelon - 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	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Bradley Collard - Pedernales Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	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	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	

Document Name	
Comment	
Suggest change to ¨To a Management Interface of Shared Cyber Infrastructure protected by an ESP¨. As management interface of target SCI should be located inside ESP and SCI outside ESP should not be in scope. Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees and changed the definition to "To a Management Interface" and moved all scoping to the standard within the Applicable Systems and Requirement Parts. CIP-005 R1.3 was rewritten to incorporate the security objective of protection of the configuration of ESPs and SCI, leaving the method to the entity.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	

2. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No: Application Containers need to be defined with additional clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA.	
Bradley Collard - Pedernales Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
PEC would like to see the SDT provide clarity regarding virtual machines on a TCA being treated as software, however a VCA running on an SCI is not software, but a CA.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of a VCA on a TCA as software.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
The phrase “actively remediated in an environement” in the PCA and VCA definitions needs to be clarified; additional information on the meaning of that phrase that was included in the technical rationale could be utilized to clarify the definitions. For CIP-003, Attachment 1, Section 4, request confirmation that, while this Section has no updates, this Section’s scope is being expanded because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification and an example of remediation and isolation. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1. It has been updated to include SCI as a conforming change.	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	
See comments from question 1.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1. It has been updated to includes SCI as a conforming change.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro appreciates the opportunity to review and offers the following comments. PCA definition needs clarification. The second bullet refers to a cyber asset being remediated in an isolated environment. It is unclear what remediation and isolation is required. An use case and example would be helpful to explain the intent here.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the updated CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification and an example of remediation and isolation.	
David Jendras - Ameren - Ameren Services - 3	

Answer	No
Document Name	
Comment	
Ameren believes that in the BCSI definition, Shared Cyber Infrastructure should be put in parentheses so that it's clear that SCI is a part of BCSI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the updated BCSI definition, modified to remove the first reference to SCI. It was determined that the threat is to the BCS, and that would extend to any SCI supporting it without having to expressly include it, as shown in the example.	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1. It has been updated to include SCI as a conforming change.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1. It has been updated to include SCI as a conforming change.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP supports all proposed definitions with the exceptions of "Cyber Assets" and "Interactive Remote Access (IRA)". Our comments are specified below: • **Cyber Assets**: The SDT added "*Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets*" to the definition of Cyber Asset. AEP suggests deleting the added sentence since it adds more confusion to the definition and it is included in the VCA definition. • **Interactive Remove Access (IRA)**: Please see our response under Question #1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA. See the response to your comments on Q1.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No

Document Name	
Comment	

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes. Further, introducing Shared Cyber Infrastructure (SCI) and Management Interface increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and "high-water marking" them with the highest identified impact rating BCA/VCA, EACMS, or PACS, and creating a BCS.

Further, the ideology surrounding "remediation VLANS" should be revisited to understand the risks posed by implementing such an environment. The complexity required to balance these pooled resources using affinity rules or logical boundaries to disallow different impact levels of VM guests from running on the same physical resources could be high. RF believes that the rationale put forth by the Standards Drafting Team for a "remediation VLAN" and the use of automation of security controls poses additional risks that can be mitigated through the use of Transient Cyber Assets (TCAs) in CIP-010 to accomplish the same vulnerability assessments and updates (OS patches, AV updates, etc.) without the complexity or risk associated with having to identify and unidentify PCAs as they are taken out and placed into service in the production network.

Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT disagrees as many will not vote to approve terms (particularly technology terms) and definitions in a vacuum with no context as to how those definitions will be used. Also, at times terms are created to match the requirements, such as IRA. Many may say that the IRA definition is too restrictive. However, it is defined so that it matches scenarios where the CIP-005 R2 requirements can be met without affecting functionality or reliability of systems.

The inclusion of "remediation VLAN" language is an attempt to address a current risk, based on the order of operations in the use of these tools. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification of the treatment of "remediation VLANS."

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

Answer	No
Document Name	
Comment	

The current definition of “Management Interface” still appears to be a bit unclear. It seems to exclude the management interface of a switch inside the Electronic Security Perimeter. NRG recommend changing the third bullet of the definition from “Configures an Electronic Security Perimeter” to “Configures a network device.” Additionally, the proposed “Protected Cyber Assets” definition could be read to include any Virtual Cyber Asset that shares physical CPU or memory, despite the addition of “resources”. We believe the intent of the drafting team to be sharing virtual CPU or memory. If so, the definition should be clarified to read, “any Virtual Cyber Asset sharing the same CPU or memory allocation.”

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The SDT modified the third bullet of the definition of a management Interface to provide additional clarity. The SDT intends this to be looked at on a physical level. Host affinity is the concept that has been continually discussed, which creates an affinity set within a cluster based on individual physical devices.

Kristine Martz - Amazon Web Services - 7	
Answer	No
Document Name	

Comment
AWS agrees with the following proposed definition changes but asks the SDT to consider including the items suggested below in implementation guidance to support entities in adopting the revised definitions: **Interactive Remote Access (IRA):** AWS asks the SDT to consider including the meaning of system-to-system communications in implementation guidance to support entities with implementing the revised IRA definition. We suggest including elements such as where the system-to-system communication originates – inside or outside of the Electronic Security Perimeter (ESP). **Management Interface:** AWS asks the drafting team to consider clarifying the meaning of “administrative interface.” For example, the SDT could clarify if “administrative interface” is intended to include Graphical User Interfaces (GUIs), Command Line Interfaces (CLIs), Software Development Kits (SDKs), and/or Application Programming Interfaces (APIs). **Virtual Cyber Asset (VCA)**: AWS asks the SDT to consider including the meaning of “dormant file-based images” in implementation guidance to support entities with implementing the revised VCA definition. Additionally, AWS suggests including guidance to ensure that security controls are in

place for dormant file-based images to mitigate vulnerabilities. For example, guidance that includes verification that required cyber security controls are in place prior to using the file-based image in production. AWS does not agree with the following proposed definition: **Transient Cyber Asset (TCA):** The modification to the Transient Cyber Asset definition that allows virtual machines running on a physical TCA to be treated as software on the device should be reconsidered. As written, an entity may not apply the appropriate security controls to the virtual machines running on physical TCAs. Entities should be monitoring the state of the virtual machines running on their physical hardware for security issues. We propose removing the language "Virtual machines hosted on a physical TCA can be treated as software on that physical TCA" from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. See the updated CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification of the treatment of VCAs on physical TCAs.

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	

Comment
The current definition of "Management Interface" still appears to be a bit unclear. It seems to exclude the management interface of a switch inside the Electronic Security Perimeter. NRG recommend changing the third bullet of the definition from "Configures an Electronic Security Perimeter" to "Configures a network device." Additionally, the proposed "Protected Cyber Assets" definition could be read to include any Virtual Cyber Asset that shares physical CPU or memory, despite the addition of "resources". We believe the intent of the drafting team to be sharing virtual CPU or memory. If so, the definition should be clarified to read, "any Virtual Cyber Asset sharing the same CPU or memory allocation."

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The SDT modified the third bullet of the definition of a management Interface to provide additional clarity. The SDT intends that this be looked at on a physical level. Host affinity is the concept that has been continually discussed, which creates an affinity set within a cluster based on individual physical devices.

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

Comment
The definition of Protected Cyber Asset carries with it an implicit requirement with the CPU and memory clause. The implication of the requirement is that a VM that is not a Protected BES Cyber Asset may not share CPU and memory with a BES Cyber System. If out-of-scope VM inadvertently shares CPU and memory with a BES Cyber System, then it suddenly becomes a PCA by definition and has instantly violated the majority of the CIP requirements. This is similar to the issue with Intermediate System that was corrected in this draft. Chelan recommends removing the CPU and memory sharing clause and adopt the suggested language in Q4 for CIP-007 R1.3, a requirement that a BCS/PCA may not share CPU and memory with non-BCS/PCA of the same impact level. That would change an inadvertent resource sharing incident into a single violation of CIP-007 R1.3 rather than violating all the requirements that have PCA as an Applicable System. Please see the response to question 4 for suggested language.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The SDT does not agree that the PCA definition imposes implicit requirements, but rather that there are consequences on the placement of VMs. The interaction of the PCA definition with the CIP Requirements has consequences for any item that meets the PCA definition, and this is intentional.

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	

Comment

WEC Energy Group has a continued concern with the newly defined term "Management Interface". Based on the rationale, it is understood why the need to define these interfaces exists. However, this definition differs from the virtual concept and extends to application functionality tools which, in our opinion, is outside of the intended scope of the Project. Thus bringing additional devices into scope even for those entities that are not using virtual machines. Proposing the SDT remove the 3rd bullet from the definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT modified the third bullet of the definition of a management Interface to provide additional clarity. The third bullet of the Management Interface definition, "• Configures an EAP", includes physical devices that can create Virtual Local Area Networks (VLANs) which applies virtualization techniques to the network infrastructure. Further, the SDT contends that the third bullet is necessary to deal with the additional complexity that Zero-Trust architectures bring to the concept of an ESP and EAP.	
Tim Kelley - Tim Kelley 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; - Tim Kelley, Group Name SMUD / BANC	
Answer	No
Document Name	
Comment	
While updating the definition of EAP for virtualization and to accommodate zero trust architectures, it would be good to also not refer to a “Cyber Asset interface,” as the EAP could be a zone-based implementation, transparent firewall, a single physical interface, multiple physical interfaces, sub interfaces (virtual SVI) or a port channel/group. The term Cyber Asset “interface” is too restrictive. We recommend the SDT change the definition to “An electronic access or policy enforcement point on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs.”	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The EAP definition is created with two ways to meet the definition. Either as a Cyber Asset Interface, for backwards compatibility, or as a policy enforcement point to accommodate Zero-Trust.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	No
Document Name	
Comment	

Manitoba Hydro thanks the drafting team for considering all comments and implementing changes to the definitions. Manitoba Hydro is in support of the changes to most definitions and the new definitions. For the updated definition of **Electronic Access Control or Monitoring Systems (EACMS)** it appears that the scope has inadvertently been increased with the "SCI" wording. The definition includes Cyber Assets… that perform electronic access control or electronic access monitoring of… SCI. The definition for SCI includes systems that host EACMS and PACS and systems that provide storage resources to EACMS and PACS. The scope of an EACMS would therefore increase to include systems that provide electronic access control and monitoring for SCI supporting EACMS and PACS, however systems providing electronic access control and monitoring directly for EACMS and PACS are not in scope. The definition is the only place where the scope of EACMS is set.

The following wording is suggested:

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s), BES Cyber Systems or SCI supporting applicable Cyber Assets. This includes Intermediate Systems.

Manitoba Hydro also notes a minor clarification in the new definition of Management Interface. It referest to deploying "SCI", this should actually refer to the VCA hosted on the SCI:

An administrative interface that:

• Controls the processes of initializing or deploying VCA hosted on SCI or

Controls the process of configuring Shared Cyber Infrastructure; or

• Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or

• Configures an Electronic Security Perimeter.

Additionally the definition for VCA includes the term “virtual machine”. This is a technology specific term and excludes some potential instances of VCA such as virtualization used in the CISCO Nexus platform. This can be resolved by removing the following wording: “currently executing on a virtual machine”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT appreciates the clarity brought to the concern around the inclusion of SCI as a target of the controls found in the EACMS definition as it was in Draft 4. The EACMS definition was modified to address this concern.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
In the proposed definition of “Cyber Asset”, the definition of “application container” versus VCA is unclear. The term “container” used in this definition needs further clarification. In the proposed definition of “Management Interface”, the definition of “administrative interface” is unclear. The term “administrative interface” used in this definition needs further clarification. In the proposed definition of TCA, removal of the qualifier “directly” may inappropriately expand the scope of the requirement to include devices connecting via IRA or Intermediate System.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA. The SDT contends the bullets following the term "administrative interface" in the Management Interface definition are the clarifying qualities that define the term, without requiring a formal definition for "administrative interface", which could cause more confusion than clarity for industry.	

Additionally, the TCA definition was modified in regards to network connectivity for clarity that applies to the removal of the term "directly".	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
Definition of VCA: NST believes the proposed definition of VCA should more closely resemble the existing definition of "Cyber Asset" or, better still, be eliminated altogether. The existing definition of "Cyber Asset" could be easily "unbound" from "hardware" with this or a similar modification: Change from, "Programmable electronic devices, including the hardware, software, and data in those devices" to, "Hardware-based or virtual programmable electronic devices, including the software and data in those devices." Definition of TCA: NST considers the statement in the proposed definition of TCA, "Virtual machines hosted on a physical TCA are treated as software on that physical TCA" to be oddly inconsistent with the proposed definition of VCA. Furthermore, we disagree with the SDT's opinion that if a physical TCA hosts one or more virtual TCAs, there should be no need to track and manage each individual physical and virtual device. Definition of ESP: NST believes the proposed new part of the current ESP definition, “or a logical boundary defined by one or more EAPs” is redundant and unnecessary. We therefore recommend maintaining the currently approved ESP definition. Definition of ERC: NST believes the use of the word, "through (an ESP)" has the potential to cause confusion over what kind of routable communications qualify as ERC. ERC to or from a Cyber Asset should be clearly defined as "through" an ESP boundary or access point, not "through" an ESP (the online Merriam Webster dictionary defines "through" as "a function word to indicate movement into at one side or point and out at another and especially the opposite side of // 'drove a nail through the board'"). NST believes the existing definition of ERC can and should be retained as-is. Definition of EAP: NST believes the proposed definition of EAP is problematic in two respects. First, we believe it could be interpreted to mean an EAP should control all routable communication between a BCS and any other Cyber Asset regardless of whether that "other" device is within or outside of the same ESP protecting the BCS. Second, we believe the SDT should better define "policy enforcement point," lest Responsible Entities, Regional Entities, and NERC develop their own conflicting definitions.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT looked at combining the CA and VCA concepts in the early stages of this project and determined that there were challenges with that approach. First, if virtual based, then the hardware would not be included. Second, the inability to target controls specifically at the virtual versions of things. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of a VCA on a TCA as software, explanations for ESP, and EAP.	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
Greater clarity is needed regarding Cyber Assets, CIP Systems and Cyber Systems. The differences between these terms should be made more explicit, overlaps should be eliminated, and redundant terms should be eliminated also.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP System has been removed as a proposed definition. Cyber Systems is simply a term as shorthand instead of having to reference all the forms that something can have. Refer to the CIP Definitions and Exemptions Technical Rationale document for further clarification.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. See response to EEI.	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
"Management Interface" – the language of the definition still leaves ambiguity of interfaces on other CAs, for example vCenter. It is understood that the intent of the SDT was to only include interfaces on applicable CAs, which could leave those unprotected by the standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See the updated CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the Management Interface definition.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the modified definitions used in the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes

Document Name	
Comment	
• NextEra Energy (NEE) encourages the SDT to enhance the clarification of bi-directional routable communication with IRA and ERC. Entities will need to clarify their implementation of bi-directional for routable communications. • Is requiring authentication to a local network or different VLAN considered a logical break?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The definition of IRA was updated to include "bi-directional" in the latest draft after the SDT determined the concept was no longer included by way of the reliance on the External Routable Connectivity definition and is an integral part of Interactivity.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the modified definitions that will be used for the CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for the hard work in developing these definitions.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments and support. See response to EEI.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE recommends consistent use of “Shared Cyber Infrastructure (SCI)” throughout the definitions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made some modifications to the use of the term Shared Cyber Infrastructure in the Draft 5 definitions.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
The only disagreement with the proposed defintions is for the CIP Senior Manager. The updated definition for CIP Senior Manager could cause some confusion because it is broad and appears to apply to all the CIP Standards, even though CIP-012 and CIP-014 do not have CIP Senior Manager requirements or responsibilities. An alternate wording could be “…. continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards in which the CIP Senior Manager has responsibilities"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT contends the original creation of the term CIP Senior Manager applied across all CIP Standards at the time, and that the role has responsibility and authority over the implementation of all CIP Standards.	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE recommends consistent use of “Shared Cyber Infrastructure (SCI)” throughout the definitions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made some modifications to the term Shared Cyber Infrastructure in the Draft 5 definitions.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the modifications to the definitions, however, would like additional clarity on the meaning of “application container” which is used within the definitions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern agrees with the proposed changes of the CIP standards definitions. Suggestions for updates have been listed below.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	

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	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 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	
Israel Perez - Salt River Project - 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	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is concerned the proposed definition of Electronic Access Point (EAP) is ambiguous. Texas RE believes the SDT's intent was to write a definition that applied to communications between BES Cyber Systems and PCAs and Cyber Assets not protected by the same ESP. The proposed definition as written, however, could be interpreted to mean that EAPs are only applicable when controlling communication between a BCS and its PCAs. The proposed language as written could also be interpreted to mean "An electronic policy enforcement point" or "a Cyber Asset interface on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs."

It could also be interpreted to mean "An electronic policy enforcement point" or "a Cyber Asset interface on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs.

For clarification, Texas RE recommends the following definition:

An EAP is:

- A Cyber Asset interface on an EACMS; or
- An electronic policy enforcement point

that controls routable communications between Cyber Systems protected by an ESP and:

- one or more Cyber Systems that are not protected by an ESP; or
- one or more Cyber Systems that are protected by a different ESP.

Likes 0	

Dislikes 0	
Response	
Thank you for your comments. See the updated EAP definition in Draft 5, which clarifies that it is controlling access to or from one or more BCS or their associated PCA.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	
Document Name	
Comment	
For definition of Transient Cyber Asset (TCA): Reconsider the wording of the sentence ¨ Virtual machines hosted on a physical TCA are treated as software on that physical TCA¨. The language used leaves room for misinterpretation and allows entities to use VM on physical TCA to bypass implementing security controls in the VM. VM image security should be verified prior to execution on TCA. For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been updated to include SCI as a conforming change.	

3. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Disagree with adding R1.6 to CIP-005 as CIP-005 is written for protections of logical devices and data. This should be restored back to CIP-006 R1 Part 1.10.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT feels that R1.6 consolidates requirements together and removes the possibility for double jeopardy.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. 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.	
Likes 0	
Dislikes 0	
Response	

Thank you for your response. R1.3. The SDT has made this requirement more objective to clearly define what is it is intended to accomplish	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. 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.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response . The SDT made this requirement more objective to clearly define what is it is intended to accomplish.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern does not agree with the proposed change in Part 1.3. The way EACMS is written, it suggests that it includes all forms of EACMS and is too broad. The term “EACMS that enforce an ESP” is not bound to firewalls and switches with VLANs, in other words EACMS that enforce network segmentation. Domain Controllers for example can help “enforce” an ESP in determining who can and can’t cross the ESP. It is not clear, in that case, what the “Management Interface” of a domain controller EACMS is, nor can routable protocol be restricted to it if its used to authenticate users. The original approved standard lists Electronic Access Points for High and Medium BCS which more aligns with equipment within an ESP. Southern suggests considering the use of EAP as the object of this requirement to clarify the scope.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT made this requirement more objective to clearly define what is it is intended to accomplish.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes modifications to CIP-005 should be limited to conforming changes only.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT maintains modifications are necessary for CIP-010 and has not limited proposed modifications to conforming changes. The SDT focused more on objective type language versus a prescriptive list. At this time, the SDT does not plan to separate virtualization requirements from the existing requirements. Project 2016-02 is not just about enabling the CIP Standards for virtualization and opening the toolbox for this option, but rather to remove encumbrances while maintaining security and backwards compatibility as key objectives. The existing baseline attributes are administratively burdensome and serve as a disincentive to virtualize, even where virtualized solutions may be more secure. Additionally, the existing construct does not lend well to a virtualized environment. The proposed modifications shift the focus from a documentation burden to security value by requiring the authorization of change instead of the update of documentation 30 calendar days after a change. The order of operations may also be different in a virtualized environment, requiring adjustments to Requirement R1, which seems to prescribe an order of 1) identify security risk, 2) authorize, 3) implement, 4) verify, remediate, reverify. For example, in a virtualized environment using Remediation VLANs the order might be 1) authorize, 2) identify security risk, 3) remediate and verify, 4) implement; without modifications entities may not be able to use features like Remediation VLANs. The prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. The purpose is to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...". The changes then require authorization per Requirement R1 Part 1.1, and which changes to high impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA, and SCI supporting an Applicable System in Requirement R2 Part 2.1 are then subject to the monitoring requirements in Requirement R2 Part 2.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way how an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear. Additional rationale and use case examples for these changes can also be found in the TR.	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
There is insufficient clarity provided within the proposed terms to ensure consistent understanding and implementation of “Management Interface”. See response to #2 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDTreworded R1.3 around Management Interfaces to be more objective.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA does not support the expansion of R1, Part 1.6 to include the protection of data traversing communications links. Expansion to communications links does not consider devices that cannot meet this criterion. Putting communication links in scope would increase costs and maintenance activities, and would require re-architecture of links. Additionally, Exemption 4.2.3.3 maintains the communications exemption for the equipment on the communications link in a ‘super-ESP’, whereas an encryption requirement when traversing multiple geographic locations would increase security for these super-ESPs. BPA suggests reverting to the Draft 3 language for R1, Part 1.6. BPA does not agree with the requirement to mitigate risk represented by sharing memory resources in R2, Part 2.6.1. The theoretical risk represented by CPU-sharing is not high enough to mandate the significant re-architecture required to adequately separate CPU usage as specified in Part 2.6.1. BPA recommends allowing the continued use of shared resources to allow entities the flexibility to balance risk mitigation with resources, maintenance and cost of maintaining the grid.	
Likes 0	
Dislikes 0	

Response
Thank you for your response. 1.6 The SDT feels the objective for the level of protection in the requirement is appropriate. This covers expansion of an ESP outside of a PSP or between sites (Super ESP). The requirement language is worded to be backwards compatible with approved versions of CIP-006 R1.10. The proposed Exemption 4.2.3.3 is for equipment "between" the devices providing encryption, not for the devices themselves. 2.6.1 Now 2.6 -The SDT modified the Intermediate System affinity requirement to "Not share CPU or memory resources with any part of a high or medium impact BCS."

Tim Kelley - Tim Kelley 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; - Tim Kelley, Group Name SMUD / BANC	
Answer	No
Document Name	
Comment	
CIP-005 R1.2 does not state that there must be a justification for the need of routable protocol communication except for in the Measures column. We recommend the SDT change the wording from permit only needed routable protocol communications, and deny all other routable protocol communications “through the ESP” to “into identified ESP(s).” ERC is defined as external routable ***connectivity***, but the requirement is for external routable ***communications***. This is another instance of the inconsistent use of routable protocol qualifiers. In the Measures column of CIP-005 R1.2, the Measure “Physical isolation of an ESP,” is confusing. The need to use routable “protocol” communications in the CIP-005 requirements is confusing. It makes it sound like routable ***protocol*** communications is something different than routable communications. You cannot have routable communications without a routable protocol unless you encapsulate the non-routable protocol. This current wording may support excluding serial communications that are encapsulated and transported via a routable protocol. It would be less ambiguous if the SDT drops the word “protocol” from routable protocol communications and just used “routable communications.”	

For CIP-005 R1.5, we recommend the SDT add a “except during CIP Exceptional Circumstances” clause to the requirement (similar to the clause added to CIP-004 R3.5). There can be multiple single points of failure impacting the ability to detect known or suspected malicious IP communications. A logging server, line card, power source, management console or SIEM could fail resulting in an immediate potential instance of non-compliance. Many of these solutions require port mirroring and there are limitations to mirroring the same source networks to multiple destination interfaces. This creates a scenario where a failed patch or unexpected hardware failure would immediately result in a potential instance of non-compliance creating unnecessary administrative burden. One solution to solve this would be to use a SPAN aggregator that splits the SPANS to two different security devices (like an IDP), but this too creates a single point of failure that during a patch, reboot or any system failure, would automatically result in a potential instance of non-compliance. For CIP-005 R2.1, the SDT should change the requirement so that the Interactive Remote Access is only initiated ***from*** an intermediate System instead of ***through*** an Intermediate System so that it’s clear that encrypted communication stops at the Intermediate System and new communication is then established from the Intermediate System.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. R1.2 The SDT agrees and changed the requirement wording to add justification of need. The SDT cleaned up the use of "routable protocol" to be more consistent. Refer to Technical Rationale for further explanations. R1.2 The SDT agrees and removed "physical isolation" from the measures. R1.5 The proposed change is not within the SAR for this project. R2.1 The SDT feels that "through" an Intermediate System is more appropriate than "from" an Intermediate System as the latter implies that IRA can originate from the Intermediate System itself.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	

WEC Energy Group does not agree with the proposed edits in R1 as it references the new "Management Interface" definition of which we do not agree (see #2 response). We also note that the reference to the Electronic Access Point has been removed from the Applicable Systems column. The Electronic Access Point modified definition is suitable for referencing physical and virtual assets. Proposing the SDT leaves Electronic Access Point in the Applicable Systems column. WEC Energy Group can support the proposed edits in R2 and R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. R1.2 EAP - The SDT feels that ESP used within the requirement is proof of changes in technology such as zero trust. In a zero trust situation, the use of EAP would require the entity to document all internal ESP communications as every system would have its own EAP.	
Kristine Martz - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	
Regarding CIP-005 Part 1.4, AWS suggests not limiting authentication requirements to dial-up connections. The SDT should broaden this requirement to include other technologies (i.e. 4G, 5G, etc.). Limiting this requirement to dial-up only may inadvertently create a security gap where alternative connection methods are not required to authenticate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. This is outside the scope of this project's SAR.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

There is still 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 enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to the Standard to ensure validity of communications to Applicable Systems.

CIP-005-8 depends upon approved SCI terminology and other definitions associated with virtualization. Approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization.

There is a significant concern is that an entity could implement "logical isolation" using only a host-based firewall on essential systems that are directly connected to the internet. Thus, exposing them to greater risk as compared the requirements in place today using defense-in-depth.

Further, introducing Shared Cyber Infrastructure (SCI) increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and "high-water-marking" them with the highest identified impact rating and creating a BCS. Allowing "mixed-trust" environments within the same SCI (hypervisor) increases the complexity and management of the environment as the SDT relaxes the "high-water-marking" required to this point. In addition, complex environments are permitted where both ESP and non-ESP Cyber Assets can be commingled on the same hardware using nothing more than affinity rules and virtual networking to segregate these systems. The complexity surrounding these installations could allow for increased risks from configuration mistakes such that ESPs could contain Intermediate Systems.

Finally, there is no NERC definition of "Remediation VLAN" so therefore the Responsible Entity could keep VMs spun up and within the Remediation network for extended periods of time – without the benefit of protections from the other CIP Standards. Accidental connection to production networks before these VMs has been properly remediated could lead to security issues and introduction of malicious communications.

CIP-005 Requirement R1 Part 1.6 – to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters, does not carry a minimum level of encryption to be required. This could result in older less secure methods being used for connections leaving the data at risk. References to NIST documentation regarding minimum encryption is suggested. Further, dependence on third-party carriers to create the "super ESP" could allow encrypt-decrypt-encrypt situations that could jeopardize the required protections for confidentiality and integrity of the data.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

R2.1 The SDT feels the proposed IRA definition has enough content to clearly show that IRA must be user initiated and is not part of system to system process communications. Any system to system process communications utilizing the same network ports as IRA would not fall within the definition of IRA. The word "authorize" has been removed. Definitions vs. Standards - The SDT has determined that for draft 5, changes made to the definitions from draft 4 will only affect the standards being re-balloted in draft 5. This concern will be addressed during the next webinar. Logical isolation and Host based firewalls - The SDT crafted the language in such a way that the requirements are compatible with zero-trust type implementations, which implies all external type communications is untrusted. It will be difficult for an entity to meet all the requirements using traditional host based firewalls as they which are not centrally controlled / administered. Remediation VLAN - The SDT crafted the requirements to be compatible with additional other methods than solely remediation VLANs. SCI / Mixed usage - The SDT feels that the methodology around the requirements for SCI are crafted in order to be flexible as technology evolves such as zero trust. R1.6 The SDT crafted a technical objective requirement to protect confidentiality and integrity and feels that using outdated encryption methods does not meet the objective. Also, exemption 4.2.3.3 is crafted so that R1.6 must be under an entity's control even if a third party is being used.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3 Recommend update to Part 2.1. Remove "authorized" from "Permit authorized." Request clarification on why Part 1.3 includes "per system capability" and Part 1.2 does not.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. 1.2 The SDT does not consider "per system capability" appropriate, but excluded time sensitive communications. Regarding 1.3, not all Management Interfaces have this capability, so "per system capability" was deemed appropriate. 2.1 The SDT removed "authorize". R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3 Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.” Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. R1.2 The SDT does not consider "per system capability" appropriate. R1.3 Not all Management Interfaces have this capability, so "per system capability" was deemed appropriate. 2.1 The SDT removed "authorize". R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No

Document Name	
Comment	
Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3 Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.” Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. R1.2 The SDT does not consider "per system capability" appropriate. R1.3 Not all Management Interfaces have this capability, so "per system capability" was deemed appropriate. 2.1 The SDT removed "authorize". R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3	
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 CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3 Recommend an update to Part 2.1. Remove “authorized” from “Permit authorized.” Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments . R1.2 The SDT does not consider "per system capability" appropriate. R1.3 Not all Management Interfaces have this capability, so "per system capability" was deemed appropriate. 2.1 The SDT removed "authorize". R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3	
John Galloway – John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3. Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.” Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. R1.2 The SDT does not consider "per system capability" appropriate. R1.3 Not all Management Interfaces have this capability, so "per system capability" was deemed appropriate.	

2.1 The SDT removed "authorize". R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	2016-02_Virtualization_Unofficial_Comment_Form.docx
Comment	
GSOC requests the SDT remove references to previous requirements regarding applicable systems and instead include the content in directly with regards to applicable systems in parts 2.2, 2.3, and 2.6. In requirement 1.6, GSOC recommends allowing for the use of a combination of both physical and encryption controls at the discretion of the responsible entity for protections in the same manner as is allowed in CIP-012 standards. {C}[TK1]{C} This inclusion of physically security controls will provide more latitude for the entity to increase security while still remaining compliant rather than relying solely upon either physical or confidentiality and integrity controls. GSOC recommends using "Confidentiality and integrity controls, and/or", or an additional bullet point specifically allowing for a combination of confidentiality and integrity controls along with physical controls. In requirement 2.1, specifying 'authorized IRA' implies that all IRA must be authorized, i.e. enumerated and documented. Additionally, the 2.1 measures then require all IRA be routed through an Intermediate System, suggesting even unauthorized IRA must do so as well. This issue persists in 2.3. Requirement 2.5, 3.1, and 3.2 language on applicability should explicitly specify it applies to only SCI having vendor remote access, rather than every SCI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. R1.6 The SDT feels that the first bullet is objective and allows for either physical or logical protection. The second bullet for backwards compatibility purposes with the previous CIP-006 standards has been added. This gives the entity the option of using either bullet.	

R2.1 The SDT removed "authorized". R2.4/2.5/3.1/3.2 The SDT agrees to restore the approved applicability. 2.6.1 – Now 2.6 -The SDT modified the Intermediate System affinity requirement to “Not share CPU or memory resources with any part of a high or medium impact BCS.”

Monika Montez – California ISO – 2 – WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	No
Document Name	
Comment	
The SRC suggests that IRA definition should remain unchanged and have the specific scenarios that these definition changes are attempting to address become part of the standard requirement language. (i.e. CIP-005-8 R2).	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The changes to the IRA definition are required to meet the objectives of the SAR. Requirement type language has been removed from the definition and placed within the R2 requirements	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Tri-State mostly agrees with the definition but thinks the second bullet,"Communication that originates from an Intermediate System"under what "IRA is not" is confusing. Isn't that system to system communication?	
Likes 0	
Dislikes 0	

Response	
Thank you for your response. The SDT cleaned up the definition for IRA. The purpose "Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs" is to exempt Cyber Systems that are already within an ESP	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS would like clarification on the restriction in R2.6.2. The part could be interpreted to restrict routable communication to any other devices or to restrict communication to those specific devices through an ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT revised R2.6.2 (now 2.7) and reworded it for clarity.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying CIP-005 to allow for more flexibility in implementing future technologies while maintaining and even increasing security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, and support. See response to EEI.	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the proposed modifications to CIP-005	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Manitoba Hydro agrees with the direction of the standard drafting team. Additional clarity could be added to sub-requirement R2.4 and R2.5. The term “with vendor remote access” has been added to the “applicable system” column. The addition of “SCI supporting an Applicable System in this Part” could mean that vendor remote access to the SCI is not in scope if there is no vendor remote access to BCS, since there are two qualifiers. Manitoba Hydro suggests adding a the qualifier “Where vendor remote access is implemented,” to the “requirements” column similar to the change done for R1.4 for Dial Up access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT agrees and reverted the language back to what was previously approved.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	

Answer	Yes
Document Name	
Comment	
Chelan appreciates the SDT's work on IRA and CIP-005 and approves the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	

Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the revisions made to CIP-005 in Draft #4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the revisions made to CIP-005 for Draft 4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
William Steiner - Midwest Reliability Organization - 10	

Answer	Yes
Document Name	
Comment	
Part 1.5 – SCI is not afforded malicious communications protections like the other CA types. While we understand the desire to avoid monitoring heavy traffic like fiber-channel, there is still a real risk of malicious code over the network to/from hypervisors (and likely other SCI) Part 1.6 – Communication between geographically dispersed SCI is not applicable, thus not necessarily afforded similar protections. Part 1.6 - Including the 'Internet Protocol' qualification in the requirement could inhibit malicious communication detection for future technologies and implementations that may not use a traditional firewall and IP routing. In particular with the change from firewalls as the outer perimeter to a zero-trust implementation, there will likely be more configuration points that aren't also acting as routers, so the inherent protection from non-IP protocols offered by the separation of subnets will no longer be there and other protocols could pass.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. R1.5 The SDT has not included SCI in the Applicable Systems as it will likely be used to meet this requirement and could result in a "hall of mirrors". R1.5 The SDT made this requirement more consistent by specifying "routable protocol" and will limit communications to routable protocol at this time so that other data center protocols currently in use are not inadvertently included. R1.6 The SDT chose not to include SCI within the Applicable Systems as SCI itself may be used to provide the required protections . This may result in a gap in protection is certain situations, however the SDT feels that a majority of situations will be covered.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See response to EEI.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro agrres with the proposed changes; however, clarification is needed as follows: In CIP-005-8 Requirement 2.1 which is, "Permit authorized....". The use of the word "authorized" is creating confusion. Typically IRA through the Intermediate System is already authorized through CIP-004. SCI was already added into CIP-004 scope therefore SCI access is authorized. IRA is applicable to all asset classifications on top of SCI which is also authorized through the CIP-004 process and not at the intermediate system. BC Hydro kindly requests that the drafting clarifies the use of the term "authorized" and recommends that the drafting team consider removing the word "authorized" from the wording of Requirement 2.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT removed the word "authorize".	
Donald Lock - Talen Generation, LLC - 5	
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	
Israel Perez - Salt River Project - 6	
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	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	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	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is concerned the definitions of Cyber Asset and PCA introduce security risks in CIP-005. The definition of Cyber Asset explicitly excludes SCI from its definition, which means SCI cannot be a Cyber Asset. The definition of PCA explicitly includes Cyber Assets or Virtual Cyber Assets in the definition. SCI cannot meet either definition, which means a hypervisor cannot be dual categorized as SCI and PCA. Therefore, an SCI placed within a network protected by an ESP arguably would not be subject to CIP-005 R1.1, R1.2, R1.5, or R1.6 despite being a PCA in all but definition.

In addition, Texas RE notes that SCI supporting high and medium impact BCS have fewer network-based protections than high and medium impact BCS. CIP-005 R1.2 is applicable to high and medium impact BCS with ERC. The requirement requires that only needed routable protocol communications are permitted through the ESP. CIP-005 R1.3 is applicable to SCI supporting medium and high impact BCS. The requirement requires that only needed routable protocol communications to and from the Management Interfaces are permitted.

Additionally, Texas RE is concerned there may be means of communicating with SCI outside of the narrow scope of the Management Interface definition. For example, an FTP server would not control the process of initializing, deploying, or configuring SCI. An FTP server is not an autonomous

subsystem that provides access to the console independently of the host system's CPU, firmware, or OS. Finally, an FTP server does not configure an ESP. As such, an FTP server running on SCI would be out of scope for CIP-005 R1.3. An FTP server in this scenario could be used to exfiltrate sensitive data, such as the disk images for the BCS that the SCI is hosting. Additionally, since SCI is out of scope for CIP-005 R1.5 entities would not be required to monitor this FTP server for malicious communications between the SCI and other systems. Texas RE suggests this issue would be mitigated by implementing high watermarking practices as described in Texas RE's response in #9. Lastly, Texas RE continues to be concerned the security objective for CIP-005-6 R1 Part 1.5 is now limited to IP malicious communications with the proposed changes. With the proposed changes this would not only reduce the compliance obligations but also create a gap in security by only focusing IP malicious communications versus all malicious communications.

Likes 0	
Dislikes 0	

Response

Thank you for your response.

The SDT feels the option of mixed trust usage of SCI should be allowed as long as the appropriate protections are in place.

Definitions - The SDT chose to separate SCI from the definitions of CA, VCA, PCA and target separate specific protections on the SCI itself. This ensures the appropriate protections are placed for the applicable CA, VCA and PCA that are running on the applicable SCI, while allowing mixed trust to exist.

R1.1/1.2 - SCI may be utilized to provide network controls for the applicable systems in a zero trust environment, thus making SCI an applicable system would introduce a "hall of mirrors" issue.

R1.3 The requirement language around Management Interface was updated to be more objective.

R1.5 The SDT feels that limiting malicious communications monitoring to IP communications is appropriate. IT is including other internal data center communications currently in use such as high fiber channel SAN cannot be monitored.

R1.5/1.6 The SDT reviewed whether it was appropriate to add SCI to R1.5 or 1.6, however SCI could be used to meet both these requirements, thus a "hall of mirrors" issue would be introduced.

FTP/BCSI - Disk images of applicable systems are considered BCSI and should be protected as such. BCSI storage is currently allowed outside of an ESP. The SDT notes that some issues around FTP could currently exist and are not SCI related. FTP remote user interactive communications are covered by the requirements around IRA and non-user interactive communications are covered under system to system process communications.

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	

4. The SDT revised CIP-007 based on industry comments. 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, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	No
Document Name	

Comment

The SRC agrees with the concept of per system capability.

For Part 1.3, we recommend changing "prevention" to "risk mitigation". "Preventing" is absolute. "Risk mitigation" is flexible.

For Part 4.3, we request adding "security" to "applicable events" for consistency with Parts of R4. Update would read "Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances."

For Part 4.4, please consider rewording this requirement to accommodate entities that use the current SIEM technology which has this type of functionality built-in and no longer requires a manual review of such data sources while also addressing those that do not have this technology.

For Part 5.1 and 5.4, leaving the scope of the term "system" up to the entity, requires effort to supply a definition and document compliance with the definition. This could lead to a misunderstanding of the intent of that term. We recommend that SDT update the technical rationale to include what is meant by "system".

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the technical rationale. Additionally, the terminology was made more consistent and 4.3 was clarified to reflect application security events. The change to 4.4 is out of scope of the SAR for Project 2016-02.

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

Answer	No

Document Name	
Comment	
No, 1.3 requirement is written more like measure with the word prevent. Would suggest rewording it to "Mitigate VCA's from CPU or memory vulnerabilities that share these resources with other VCA's that are not associated with the same impact categorization." Then prevention could be one of the measures.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the technical rationale.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation.”“Prevention” is absolute. “Risk mitigation” is flexible. Perhaps “prevention” can be moved to the Measures as a suggestion/ Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles. For Part 4.3, request adding “security” to “applicable event” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT clarified the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was updated to reflect application security events.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	

Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion. Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles. For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. The update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT clarified the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was updated to reflect application security events.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
In R1.1, Ameren believes that the phrase "routable protocol network accessibility" is unclear and there should be more clarity as to what this phrase means. We are concerned an auditor might think of this phrase differently than Ameren does, so we believe more clarity around this phrase will ensure that auditors and Ameren have the same understanding as to what the phrase means. In R4.3, the phrase "per system capability" was added. Does any paperwork need to be filled out and provided to the regional entity for devices that fall into the "per system capability" classification? For example, paperwork needs to be filled out for TFEs.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT added clarity in the TR for both the phrase "routable protocol network accessibility" in 1.1 and "per system capability" in 4.3.	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion. Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles. For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was clarified to reflect application security events.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion. Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles.	

For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was clarified to reflect application security events.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion. Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles. For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was clarified to reflect application security events.	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	

Recommend removing EACMS and PACS from the applicability section. If EACMS or PACS were to reside inside an ESP they are also categorized as PCAs so they will be covered. This change will exclude other CAs in a DMZ virtual system that do not perform EACMS or PACS functions and will thus retain the backward compatibility of the standard while allow greater protection for BCAs and PCAs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement, removing EACMS and PACS.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	

Chelan believes the proposed language for CIP-007 R1.3 is overly burdensome and the required control does not reflect the actual risk of a VM escape attack. The intended controls (DRS affinity rules) listed in the measures are not intended for security control purposes, but are instead intended for resource control purposes. Because of this and the very broad applicability, they will have overly complex rulesets that introduce reliability risks where, in the event of a failure or during maintenance activities, a crucial VM may not be able to find a suitable host and crash. Given there are few if any demonstrated attacks along this threat axis, this seems to be an overreach.

Additionally, this requirement is not backwards compatible with the existing requirements. The currently effective requirements allow the mixing of EACMS and PACS VMs with out-of-scope VMs so long as the hosts themselves are classified as EACMS and PACS.

Finally, Chelan believes there is a Low Impact problem in the proposed requirement. The Applicable System is an SCI that hosts High or Medium Impact VCAs, not the actual High or Medium Impact VCAs themselves. The text of the requirement itself does not restrict itself to High and Medium and simply refers to “same impact classification”. If an SCI that hosts High or Medium Impact VCAs also hosts Low Impact BCS, the requirement is on the SCI to prevent sharing of CPU and memory between devices that are not of the same impact categorization, regardless of what that impact categorization might be. Low Impact is a different impact category from no impact, so the requirement would force the SCI to segregate Low Impact VCAs from no impact VCAs. That essentially places a requirement on Low Impact devices to not share CPU and memory with no-impact devices, so long as they are on the same SCI as a High and Medium impact VCA.

All that said, Chelan does recognize the risk of a zero day exploit along this vector and therefore, Chelan recommends this requirement should be restricted to BCAs and PCAs, and left EACMS and PACS out, which would be backwards compatible with the existing requirements and guidance. The

suggested language below would prevent devices that are within the ESP from sharing CPU and memory with devices outside the ESP or in different impact level ESPs. This would accomplish the goal of protecting BES Cyber Systems and would simplify implementation by creating three categories of devices that may not share CPU and memory, rather than potentially six. Chelan suggests the following language for CIP-007 R1.3: Applicable Systems: SCI supporting: High Impact BCS and their associated PCA; Medium Impact BCS and their associated PCA Requirement: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources, excluding storage resources, between High and Medium Impact BCS and their associated PCA, and VCAs that are not BCS or PCAs of the same impact categorization.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement, removing EACMS and PACS.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group does not agree with the proposed edits and retitling of R1. Changing the title of R1 to System Hardening implies the potential for more than just the management/monitoring of ports and services. Although "system hardening" is a best practice, it is at this time self defined and is too broad of a term to be used for CIP-007 R1 and in our opinion beyond the virtualization intent of the Project. Additionally, Part 1.1 implies ports and services in the Requirement, we understand it was rewritten in an attempt to address SCI supporting the Applicable System, however the rewrite is too broad and looses its intent of ports and services. Also note, the Measures for Part 1.1 describes the aspects of ports and services, why not use those same terms (ports and services) in the Requirement itself. Proposing the SDT leaves the title of the R1 as Ports and Services, leave R1 Part 1.1 and Part 1.2 as written and separate the SCI references included in current draft Part 1.3 into its own Requirment or Part. WEC Energy Group can support the proposed edits in R2-R5.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The reasoning behind the name change is to reflect the security objective of the entries more clearly in the table, which is to reduce a systems' attack surface. The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCA.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
As it pertains to CIP-007 R4.2, the use of the term system in the statement "per system capability" leads to subjectivity. We recommend the use of "per Cyber Asset or BSC capability" as it defines the scope of capability. Additionally, our comment from the last comment period of "If a firewall has VLANs on it for medium and low, or high and low, does that pull low impact network connection into scope because it shares the same firewall?" was not addressed by SDT as far as we know.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT added more clarification to the TR.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes modifications to CIP-007 should be limited to conforming changes only.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT is changing R1.1 so that it can incorporate newer security models, such as zero trust. The addition of R1.3 addresses the possibility of VM escape. Refer to the CIP-007-7 TR for more information	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern disagrees with the proposed changes to CIP-007 R1.3 Applicable Systems. Adding EACMS and PACS in both High and Medium Impact BCS increases the requirements for associated virtual assets. Southern agrees that for hypervisors which ALSO host BCS, the scope is appropriate, but for hypervisors that ONLY host EACMS outside of an ESP, with no BCS, it is an "anti-virtualization" incentive to dedicate hypervisors to a domain controller for example. Suggest changing the language to High/Medium Impact BCS and their associated PCA, which will keep this affinity requirement scoped to hypervisors that host BCS and anything else.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT clarified the wording of the requirement, removing EACMS and PACS.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	

See response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the revisions made to CIP-007 for Draft 4.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the revisions made to CIP-007 in Draft #4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the proposed modifications to CIP-007.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying CIP-007 to allow for more flexibility in implementing future technologies while maintaining and even increasing security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See the response to EEI.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the revised CIP-007 proposed changes.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 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), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley 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; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
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	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 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	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	

Texas RE is concerned the language: “logical network accessible ports… including port ranges or services where needed to handle dynamic ports” was removed. Both ports and services are required to gain a better understanding of where vulnerabilities can exist whether in a physical or virtualized environment. Ports and services are often used for malicious reconnaissance and lateral movement within networks. Registered Entities should understand and document why ports and services are needed for many reasons (defense in depth, zero trust, etc. concepts).

Texas RE is concerned the phrase “CPU and memory resources” in CIP-007-7 Requirement R1.3 is written could be interpreted as (CPU and memory) resources or as CPU and (memory resources). Texas RE recommends rewording the sentence so it is clear that the CPU resources and memory resources should not be shared: “the sharing of CPU resources and memory resources.”

Additionally, in order to make the language of Requirement 1.3 more consistent with other requirements in CIP-007-7, Texas RE recommends revising the existing language Requirement R1.3 to “Prevent the sharing of CPU resources and memory resources, excluding storage resources, between Virtual Cyber Assets (VCAs) that are not of, or associated with, the same impact categorization.” The technical rationale for this requirement can then explain that the requirement is needed in order to mitigate the risk of CPU or memory vulnerabilities.

Lastly, Texas RE noticed inconsistent redlining between the “redline_to_last_approved” and “clean” copies of the standard for CIP-007-7 R4.1. In the “clean” version of the standards the following language, which Texas RE agrees with reads as:

Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events

In the “Redline to Last Approved” version the phrase “and after-the-fact investigations of” has been marked for removal. Texas RE does not agree with removing this phrase from the requirement.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT clarified the wording in 1.3 and 4.1. The phrase "after-the-fact investigations of" has not been removed.

5. The SDT has used phrasing such as "SCI supporting an Applicable System from this Part" in the Applicable Systems column across many of the standards. Is it clear that this scopes the requirements for SCI to match the system(s) it hosts?	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes the phrase needs to be more specific. "Supporting" an Applicable System is too broad. BPA proposes adding SCI under the Applicable Systems column in the Requirements/Parts tables, grouping it with each appropriate impact rating similar to the way EACMS, PACS, and PCA are scoped. Additionally, the definitions for EACMS and PACS include SCI so these do not need to be accounted for. Alternatively, since the term "and their associated" is widely used in the standards, replacing the word supporting with "associated with" may be more clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the use of "SCI supporting an Applicable System from this Part" in the Applicable Systems column of the requirement, to ensure that controls relevant to the hardware portion of a physical Cyber Asset, would remain applicable to the hardware supporting the VCA used in BCS, EACMS, PACS or PCA. Clarifying updates have been added to the TR.	
Israel Perez - Salt River Project - 6	
Answer	No
Document Name	
Comment	
The phrase "SCI supporting an Applicable System from this part" is still not clear enough and needs more verbage to explain what it applies to. The phrase could also be re-written as "SCI supporting the identified Applicable System in this Part"	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT believes the use of "SCI supporting an Applicable System from this Part" in the Applicable Systems column of the requirement to ensure that controls applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA. Additional clarity has been added to the TR.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
"Part" is not a defined term, for additional clarity the drafting team could replace this phrase with "SCI supporting an Applicable System". Lastly, "Applicable System" is used multiple times in the draft CIP standards and is not a defined term or a proposed defined term. The standard drafting team may consider defining this term in the NERC Glossary of Defined Terms.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. “Part”, “Applicable System”, “Requirements”, and “Measures” are used throughout the CIP standards, in both verbiage and in the table column titles. The SDT does not find it necessary to add these to the NERC Glossary.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, Supporting an applicable system is not specific enough and could be misterupted	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT believes the use of "SCI supporting an Applicable System from this Part" in the Applicable Systems column of the requirement to ensure that controls applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA. Additional clarity has been added to the Technical Rationale.	
Donald Lock - Talen Generation, LLC - 5	
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	
Comment	
Southern agrees and appreciates the included language of "SCI supporting an Applicable System in this Part" across the many standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes

Document Name	
Comment	
AZPS agrees that the phrasing of “SCI supporting an Applicable System from this Part” is clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy believes there is some lack of understanding at our company and throughout the industry on how SCI should be categorized when they are supporting EACMS or PACS and so, Xcel Energy supports the comments of the MRO NSRF. While Xcel Energy supports clarifications, our concerns do not rise to the level of requiring us to vote no on proposed Standards with SCI as an applicable system.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. SCI is much like EACMS and PACS in that these categories of Cyber Assets do not technically have a direct impact rating, making their categorization less conducive to ‘high watermarking concepts.’ Where SCI supports EACMS and PACS (and not BCS or PCA), the SCI inherits the requirements for the collective impact ratings of each associated BCS for each of the EACMS and PACS that SCI supports. Registered Entities implementing SCI that supports both EACMS and PACS should approach categorization holistically and apply multiple categorizations and collective coverage of that supporting SCI under all applicable Requirement Parts. Registered Entities run the risk of security/compliance gaps if attempting to ‘high watermark’ to a single categorization where SCI supports both EACMS and PACS associated to varied impact levels of BCS. The applicable requirements are an aggregate of the requirements of the hosted	

Applicable Systems. See the TR for a more comprehensive explanation, including an example of a specific use case.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees the phrasing of "SCI supporting an Applicable System from this Part" in the Applicable Systems column in the Standards makes it clear the scoping is for the hosts the SCI supports.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Tim Kelley - Tim Kelley 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; - Tim Kelley, Group Name SMUD / BANC	

Answer	Yes
Document Name	
Comment	
This is fairly clear. However it would be better to see some verbiage/examples in the technical rationale related to the inclusion of “storage resources required for system functionality of one or more Cyber Assets or VCAs….” found in the second bullet of the SCI definition to limit the scope of applicability. It’s not quite clear what exactly may be pulled into scope by the wording in the second bullet and there may be an unintentional increase in applicability. CIP-007 R1.3 specifically excludes storage resources in the requirement, but in the definition of SCI, the second bullet specifically includes storage resources in the definition of SCI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See the TR for CIP-007 R1.3 for additional clarification.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes

Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the phrasing “SCI supporting an Applicable System from this Part” in the Applicable Systems column across many of the standards is clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	

Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 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	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
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	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 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	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
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	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

patricia ireland - DTE Energy - 4, Group Name DTE Energy	
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	
Daniel Gacek - Exelon - 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	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	

6. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	CIP-010 Alternate Update.docx
Comment	
ecommending maintaining the CIP-010-4 requirement to establish and maintain the baseline. Justification: While the TR does allude to the use of the baseline configuration as the "how" this requirement can be met, it is followed by stating the entity would be required to document how the baseline meets the stated security objective and references NIST SP 800-128 as a guide. Throughout NIST SP 800-128 the baseline configuration is referenced as the "secure state", specifically "*…baseline configuration for a system and associated components represents the most secure state consistent with operational requirements and constraints*" (NIST.SP.800-128, Section 2.2.2,	

pp. 21). Establishment and maintenance of a baseline configuration provides the entity with a secure starting point from which each modification can build upon.

Removing the requirement for a baseline configuration and/or requiring the entity to justify the use of the baseline appears to go against the guidance provided in NIST 800-128.

R1 Response

Part 1.1

R1.1 Document and maintain system configurations (to include at a minimum software addressing the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.)

R1.1.1 Manage changes which alter the system configuration

R1.1.2 Authorize changes to the system configuration

R1.1.3 Validate implementation of changes to the system configuration

Part 1.2

1.2.1. Prior to implementing a change to system configurations from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 andCIP-007 remain implemented as required; and

1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Part 1.3

For a change that deviates from the existing system configuration, update the system configuration documentation as necessary within 30 calendar days of completing the change.

R2 – Security Configuration Monitoring

Considering the changes made to R1 and the proposal to maintain the baseline configuration documentation requirements the following is a proposed adjustment to R1.

Response Part 2.1 *Methods to monitor at least once every 35 calendar days for unauthorized changes to the system configuration. Document and investigate detected unauthorized changes.* 1 – The language used in the requirement, specifically “settings”, will force a significant and increasing administrative burden on the Entities. The control which applies to the requirement for each of the items within CIP-005 and CIP-007 will typically contain a multitude of “settings” which enforces the configuration of the control as a collective. There is a concern that the Entity will be ‘too far in the weeds’ focusing on the numerous settings that contribute to a control thereby diverting attention from the security posture of the environment. 2 – Confirmation after implementation of the authorized/documented change of the controls which enforces the requirement in CIP-005 and CIP-007 ensures the security configuration of the applicable system was not impacted in a manner that would weaken the security posture of the applicable system.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT considered the suggestion to reintroduce the word 'baseline' so R1 would provide clarity on 'how' to meet the requirement using a 'baseline'. It was determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The SDT also maintains that the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility and provide clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to demonstrate an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", and then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	No
Document Name	
Comment	

The proposed changes to CIP-010 are SRC's gravest concern as we believe the proposed changes go beyond what was previously in the CIP standards such that they would no longer be backwards compatible. In particular, the addition of the concept of "settings changes" is overly broad; whereas the prior standard focused on changes to the baseline configuration. SRC proposes "settings changes" be modified to "configuration changes" or eliminated altogether.

For consistency, please add the term "Cyber" to security patches.

The SRC requests clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document that baselines (from previously approved Standard) track or show any changes made to applicable CIP-005 and CIP-007 security controls

The SRC requests that consistent language be used when addressing the same subject in different parts of the standard within the Requirements of Parts 1.1 and 1.3. Examples of this include the following:

- *Part 1.1 provides what is included in software*
- *Part 1.3 distinguishes some of 1.1 apart from software*
- *Part 1.1 starts with "Control the implementation of intended changes to software, or intended changes to settings . . ."*
- *Part 1.1 also says "Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.*
- *Part 1.3 starts with "Prior to the installation of operating systems, firmware, software, or software patches . . ."*

While we recommend that that CIP-010 R1 needs to be left "as is" as changing the requirement may present a greater compliance burden on the entity with a less clear objective/goal. The proposed changes do not increase the level of security that are currently afforded by the existing standard.

For Part 2.1, we recommend this requirement is also left "as is". The proposed requirement is overly burdensome and may require the monitoring of the entire asset, including its filesystem, registry, miscellaneous settings, accounts, etc. and is above and beyond what is currently required with little added security benefit.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT considered comments regarding the potential for confusion, perceived scope increase, or misinterpretation by use of terms like "settings". This phrasing was removed to prevent it from being interpreted as too prescriptive.

The SDT agreed with suggestions to add the word "cyber' in front of "security patches", and updated the term throughout the standards.

Regarding the need for Measures to meet the Objectives and consistency of terms, and when modifying Requirement R1, the SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain a choice for an entity to demonstrate compliance, as well as assure the virtualization components are aligned. The TR was reviewed to ensure the baseline part is clear. The SDT maintains Project 2016-02 is not just about enabling the CIP Standards for virtualization and opening the toolbox for this option, but rather the intention to remove encumbrances, while maintaining security and backwards compatibility as key objectives. The existing baseline attributes are administratively burdensome and serve as a disincentive to virtualize, even where virtualized solutions may be more secure. Additionally, the existing construct does not lend well to a virtualized environment. The proposed modifications shift the focus from a documentation burden to security value by requiring the authorization of change instead of the update of documentation 30 calendar days after a change. The order of operations may also be different in a virtualized environment, necessitating adjustments to Requirement R1, which seems to prescribe an order of 1) identify security risk, 2) authorize, 3) implement, 4) verify, remediate, reverify. For example, in a virtualized environment using Remediation VLANs, the order might be 1) authorize, 2) identify security risk, 3) remediate and verify, 4) implement; without modifications entities may not be able to use features like Remediation VLANs. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. To maintain backwards compatibility and clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. This demonstrates an entity can continue to use baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement part(s) in CIP-005 or CIP-007...", which changes then require authorization per Requirement R1 Part 1.1, and which changes to high impact BES Cyber Systems and their associated 1. EACMS; and 2. PCA, and SCI supporting an Applicable System in Requirement R2 Part 2.1 are then subject to the monitoring requirements in Requirement R2 Part 2.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
R1.1 The phrase "...could weaken configured cyber security controls.." is very general and expands the original baseline scope widely to include endless settings that could be under the review of an audit.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT considered your perspective, agrees it carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	CIP-010 Alternate Update.docx
Comment	

Recommending maintaining the CIP-010-4 requirement to establish and maintain the baseline.

Justification:

While the TR does allude to the use of the baseline configuration as the “how” this requirement can be met, it is followed by stating the entity would be required to document how the baseline meets the stated security objective and references NIST SP 800-128 as a guide.

Throughout NIST SP 800-128 the baseline configuration is referenced as the “secure state”, specifically “*…baseline configuration for a system and associated components represents the most secure state consistent with operational requirements and constraints*” (NIST.SP.800-128, Section 2.2.2, pp. 21). Establishment and maintenance of a baseline configuration provides the entity with a secure starting point from which each modification can build upon.

Removing the requirement for a baseline configuration and/or requiring the entity to justify the use of the baseline appears to go against the guidance provided in NIST 800-128.

R1 Response

Part 1.1

R1.1 Document and maintain system configurations (to include at a minimum software addressing the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.)

R1.1.1 Manage changes which alter the system configuration

R1.1.2 Authorize changes to the system configuration

R1.1.3 Validate implementation of changes to the system configuration

Part 1.2

1.2.1. Prior to implementing a change to system configurations from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 andCIP-007 remain implemented as required; and

1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Part 1.3

For a change that deviates from the existing system configuration, update the system configuration documentation as necessary within 30 calendar days of completing the change.

R2 – Security Configuration Monitoring

Considering the changes made to R1 and the proposal to maintain the baseline configuration documentation requirements the following is a proposed adjustment to R1.

Response

Part 2.1

Methods to monitor at least once every 35 calendar days for unauthorized changes to the system configuration. Document and investigate detected unauthorized changes.

1 – The language used in the requirement, specifically “settings”, will force a significant and increasing administrative burden on the Entities. The control which applies to the requirement for each of the items within CIP-005 and CIP-007 will typically contain a multitude of “settings” which enforces the configuration of the control as a collective. There is a concern that the Entity will be ‘too far in the weeds’ focusing on the numerous settings that contribute to a control thereby diverting attention from the security posture of the environment.

2 – Confirmation after implementation of the authorized/documented change of the controls which enforces the requirement in CIP-005 and CIP-007 ensures the security configuration of the applicable system was not impacted in a manner that would weaken the security posture of the applicable system.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT considered the suggestion to reintroduce the word 'baseline' so R1 would provide clarity on 'how' to meet the requirement using a 'baseline'. It was determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility and clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to demonstrate an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement part(s) in CIP-005 or CIP-007...", and which changes then require authorization per Requirement R1 Part 1.1. The measures were aligned by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
R1.3 – consistency of phrases among the requirements is necessary, For instance, in Requirement 1 part 3, the phrase used is “Prior to installation.” In other sections, however, the phrase used is “prior to the intended change” One of the two phrases should be used throughout. Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .” Part 1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”	

For Part 3.3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term? “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s. For Part 3.3, request removing “any” from the first Measures bullet because “any” is a scope concern where “any” is interpreted as “all.” For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT was mindful to assure alignment of terms. The SDT revisited the Measures when making modifications to Requirement R1 Part 1.1 to assure the Measures meet the Objectives of the requirements as suggested. Also considered were comments regarding Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, the SDT made modifications to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed. The intent is to require assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented, or when failures occur and existing Cyber Assets need to be replaced. The risk is associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another, configured like the one being replaced, suggests the security posture is known as a function of the reconstruction process to build the replacement. Since the existing Cyber Asset had been previously assessed, the performance of the requirement part is not warranted. Entities can still choose to define the term ‘like replacements’ within their own programs and processes if the Registered Entity deems that necessary or a value add. The SDT removed the word "any" from the Measures for Requirement R3 Part 3.3 as requested. Regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads, “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;”, the SDT agrees with the unintended consequence that this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. The bullet was removed in response to this industry concern.	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	

Answer	No
Document Name	
Comment	
The word "setting" should be further clarified.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Regarding the potential for confusion, or perceived scope increase or misinterpretation by use of terms like "settings", the SDT agreed this would be interpreted as too prescriptive and the phrasing was removed.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	

SPP would like to understand how the significant proposed changes in CIP-010-5, specifically Requirement R1, relate to what was requested in the Project 2016-02 SAR. SPP believes that the verbiage related to SCI, containerization, and ESPs between systems with different impact ratings can be added without having to change the way that entities have to comply with CIP-010 today.

The new proposed language greatly expands the scope for CIP-010 and raises concerns for backwards compatibility with existing baseline methods, adds unnecessary complexity, and significantly increases cost with minimal security benefit. The current baseline configuration requirements have been moved to the Measures column along with additional verbiage to address virtualization. However, the control language is very broad and can lead to different interpretations depending on the auditor and uncertainty in tracking changes. Responsible Entities have demonstrated that both physical and virtual systems are capable of developing, documenting, approving, tracking, updating, and monitoring baseline configurations. For these reasons, SPP believes that the prescribed baseline configuration requirements should remain in place with the addition of specific verbiage related to virtual architecture and containerization. The baseline language supports a secure baseline configuration and represents industry best security practices.

The NIST 800-128 guidelines refer to applying the security configuration management practices that include "monitoring the configuration of systems to ensure that configurations are not inadvertently altered from the approved baseline", thus implying that baseline configuration management is key to securing a system. These guidelines further define a Baseline Configuration as, "A set of specifications for a system, or CI

within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes." This definition fits well with the currently approved verbiage in CIP-010-4 where the "set of specifications for a system" was clearly defined for the baseline and approved through change control methods. The baseline is an understanding of what the approved system configuration should be so that there is an understanding of what has changed. According to NIST, the baseline configuration should represent a secure state of the system while also maintaining a "cost-effective and functional support of mission and business processes". The updated control verbiage does not reference a baseline configuration and does not adhere to a cost-effective support of security best practices, therefore creating a risk to demonstrate compliance.

The following proposed language for CIP-010-5, Requirement R1, Part 1.1, could address virtualization while also maximizing backwards compatibility:

Develop a baseline configuration, individually or by group, which shall include the following items:

1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;

1.1.2. Any commercially available or open-source application software (including version)

intentionally installed including application containers;

1.1.3. Any custom software installed, including application containers;

1.1.4. Configuration that modifies network accessible logical ports or network accessible services on an Applicable System;

1.1.5. Any security patches applied;

1.1.6. SCI configuration of host affinity control between systems with different impact ratings;

1.1.7. Changes to configurations or settings for an ESP between systems with different impact ratings; and

1.1.8. Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT maintains Project 2016-02 is not just about enabling the CIP Standards for virtualization and opening the toolbox for this option, but rather the intention to remove encumbrances, while maintaining security and backwards compatibility as key objectives. The existing baseline attributes are administratively burdensome and serve as a disincentive to virtualize, even where virtualized solutions may be

more secure. Additionally, the existing construct does not lend well to a virtualized environment. The proposed modifications shift the focus from a documentation burden to security value by requiring the authorization of change instead of the update of documentation 30 calendar days after a change. The order of operations may also be different in a virtualized environment, requiring adjustments to Requirement R1, which seems to prescribe an order of 1) identify security risk, 2) authorize, 3) implement, 4) verify, remediate, reverify. For example, in a virtualized environment using Remediation VLANs, the order might be 1) authorize, 2) identify security risk, 3) remediate and verify, 4) implement; without modifications entities may not be able to use features like Remediation VLANs. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. To maintain backwards compatibility and clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to demonstrate an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement part(s) in CIP-005 or CIP-007...", which changes then require authorization per Requirement R1 Part 1.1, and which changes to high impact BES Cyber Systems and their associated 1. EACMS; and 2. PCA, and SCI supporting an Applicable System in Requirement R2 Part 2.1 are then subject to the monitoring requirements in Requirement R2 Part 2.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear, and additional examples of these changes can be found in the TR.

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	No
Document Name	

Comment

While we appreciate the thoughtful proposal of a less prescriptive requirement for CIP-010, there are many unintended consequences with the expansion of scope in the currently proposed language. The word “settings” scopes too many possible features into CIP-010 that do not necessarily have a compelling security value. Additionally, the concept of a baseline is foundational in NIST SP 800-128 . It is possible to have less prescriptive requirements that advance the intention of CIP-010 and its security objectives,while maintaining true backward compatiability.Here is our alternate proposal that we have worked with Exelon to craft:

R1.1 Document and maintain system configurations (to include at a minimum software addressing the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.)

R1.1.1 Manage changes which alter the system configuration

R1.1.2 Authorize changes to the system configuration

R1.1.3 Validate implementation of changes to the system configuration

R1.2.1. Prior to implementing a change to system configurations from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 andCIP-007 remain implemented as required; and *R1.2.2. Document the results of the testing, and if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.* *R1.3 For a change that deviates from the existing system configuration, update the system configuration documentation as necessary within 30 calendar days of completing the change.* *R2.1 Methods to monitor at least once every 35 calendar days for unauthorized changes to the system configuration. Document and investigate detected unauthorized changes.*

Likes 0	
Dislikes 0	

Response
Thank you for your comments. Regarding the potential for confusion, or perceived scope increase or misinterpretation by use of terms like "settings", the SDT agreed this would be interpreted as too prescriptive and the phrasing was removed. The SDT considered the suggestion to reintroduce the word 'baseline' so R1 would provide clarity on 'how' to meet the requirement using a 'baseline'. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility and clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to demonstrate an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", and which changes then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	
Comment	

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. The entity may need to document its baselines (from previously approved standards) when addressing its CIP-005 and CIP-007 security controls.

Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in the software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to the software or intended changes to settings . . .” Part 1.1 also says “Changes to the software include the installation, removal, or update of the operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”

For Part 3.3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term? “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s.

For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.”

For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Regarding the need for Measures to meet the Objectives and consistency of terms, and when modifying Requirement R1, the SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance, as well as to assure the virtualization components are aligned. The TR was reviewed to ensure the baseline part is clear.

The SDT made modifications to assure consistent use of terms instead of the use of similar terms like “software patches” and “security patches” to further remove any concerns of unintended nuances from using synonymous terms interchangeably; cyber security patches is now the term used throughout.

Also considered were comments regarding Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, the SDT made modifications to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed. The intent is to require assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented, or when failures occur and existing Cyber Assets need to be replaced. The risk is associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another, configured like the one being replaced, suggests the security posture is known as a function of the reconstruction process to build the replacement. Since the existing Cyber Asset had been previously assessed, the performance of the requirement part is not warranted. Entities can still choose to define the term 'like replacements' within their own programs and processes if the Registered Entity deems that necessary or a value add. The SDT removed the word "any" from the Measures for Requirement R3 Part 3.3 as requested. Regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads, "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;", the SDT agrees with the unintended consequence that this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. The bullet was removed in response to this industry concern.
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment
BC Hydro appreciates the opportunity to review and offers the following comments: 1. CIP-007 and CIP-005 Standards were modified to explicitly call out specific controls related to SCI (e.g. CIP-007 R1.3 / CIP-005 R1.3) but in CIP-010 R1 it is not written with the same clarity. For example, in CIP-010-3 R1.1 measures provided are not truly applicable to non SCI CIP-007 and CIP-005 controls. Operationally they differ greatly from non-SCI classified assets. Similar to the pattern followed in CIP-005 and CIP-007 changes, BC Hydro proposes to call out in a separate requirement SCI controls that need to be evaluated. 2. The inclusion of the following "... or intended changes to settings that could weaken configured cyber security controls required by CIP005 and CIP-007" makes the Requirement R1.1 of CIP-010-3 unclear. It is indicative that this Requirement will only apply if the change in settings has an effect on the configured CIP-007 and CIP-005 controls. However the expected scope of changes in settings need clear direction and guidance. Some pertinent use case examples and clear direction is needed here.

Likes 0	

Dislikes 0	
Response	
Thank you for your comments. The SDT focused more on objective type language versus a prescriptive list and does not plan to separate virtualization requirements from the existing requirements at this time. The SDT considered your perspective, agreed it carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren believes that R1.1 is too large of a requirement and should be split up into multiple smaller requirements. In R2.1, Ameren would like examples of "settings that could weaken configured cyber security controls," because this could be left up to interpretation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT believes splitting R1.1 into multiple requirements could potentially create double jeopardy across requirements. However, the Part for verification of security controls was separated from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur as a part of the change authorized in Part 1.1. The SDT also considered your perspective the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed the language and refocused the requirement on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	No
Document Name	
Comment	
Concerns regarding backward compatibility. And how compliance on existing practices will be assessed following the proposed change. Specifically how current practices related to “Live operating system and software executable only from read-only Media” can still need the intent of Section 1.3 without subjectivity inherent in the “other mitigation methods” option. Request adding of technical rationale (i.e. the intent of the change) for Attachment 1 Section 1.3. in particular explanation on the bullet that was added, i.e. “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution”. Support comment from NPCC RSC. Reiterated here: “For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT considered comments regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads, “Controls that maintain the state of the operating system and software such that it is in a known state prior to	

execution;". The SDT agrees with the unintended consequence that this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. The bullet has been removed in response to this industry concern.	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No
Document Name	
Comment	

For requirement 1.1.2, we suggest to simply write, "Verify the required cyber security controls remain implemented". There is confusion as to why "…as required as a part of the change" adds to the requirement.

However, the newest version is closer to what is done by industries. Old version address the case when a plan made its own programs in assembly language. Now, it's more representative of the real world when third-party software executables are buy and install in systems.

1) It is unclear if Management Interface of Cyber System is in scope for CIP-010

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document that their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls.

Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with "Control the implementation of intended changes to software, or intended changes to settings . . ." Part 1.1 also says "Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches." Part 1.3 starts with "Prior to the installation of operating systems, firmware, software, or software patches . . ."

For Part 3,3, request clarification on the first Requirement bullet – "Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System." The term "like replacement" is an undefined term. Does the SDT intend for the entity to define this term. "Configuration of the previous" implies a baseline that was not specified. As written, the entity's interpretation may be different than the auditor's.

For Part 3.3, request removing "any" from the first Measures bullet because any is a scope concern . . . where any is interpreted as "all."

For 1.3 in Attachment 1, recommend changing this new bullet from "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;" to "provide valid mitigation" since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Regarding Part 1.1.2, and the unintended implication that that entities must verify all “required cyber security controls remain implemented as required”, the SDT separated the requirement for verification of security controls from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur 'as a part of the change' authorized in Part 1.1, and scoped those verification actions to what was relevant to the changes so a complete compliance check for CIP-005 and CIP-007 is not required. Yes, the Management Interface of a Cyber System is in scope for CIP-010. CIP-005 contains specific requirements for the controls that must be implemented for a Management Interface where the Glossary term is used within the Requirement or Requirement Part in CIP-005. A Management Interface is a component of a Cyber System, so where changes to the Management Interface's implemented cyber security controls serving the requirements in CIP-005 occur, those changes would be subject to CIP-010 requirements. The SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The SDT agrees the use of "AND" vs "OR" in relation to the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity." Also considered were comments for Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, modifications were made to shift the focus on “previously assessed configuration” as the reason why an active vulnerability assessment need not be reperformed. The intent is to require active vulnerability assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented or when failures occur, and existing Cyber Assets need to be replaced. The risk is associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another Cyber Asset that has been configured like the one being replaced suggests the security posture is known as a function of the reconstruction process to build the replacement, and because the existing Cyber Asset had been previously assessed, thereby not warranting the performance of the requirement part. Entities can still choose to define the term ‘like replacements’ within their own programs and processes if the Registered Entity deems that necessary or a value add. The word "any" was removed from the measure per your comment. Regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;”, the SDT agrees this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. This bullet was removed in response to this industry concern.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No

Document Name	
Comment	
Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls. Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .” Part 1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .” For Part 3.3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term. “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s. For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.” For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Regarding the need for Measures to meet the Objectives and consistency of terms, and when modifying Requirement R1, the SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance, as well as to assure the virtualization components are also aligned. The TR was reviewed to ensure the baseline part is clear. The SDT made modifications to ensure consistent use of terms instead of the use of similar terms like “software patches” and “security patches” to further remove any concerns of unintended nuances from using synonymous terms interchangeably; cyber security patches is now the term used throughout. Also considered were comments for Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, modifications were made to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed. The intent is to require active vulnerability assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented or when failures occur, and existing Cyber Assets need to be replaced. The risk is	

associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another Cyber Asset that has been configured like the one being replaced suggests the security posture is known as a function of the reconstruction process to build the replacement, and because the existing Cyber Asset had been previously assessed, thereby not warranting the performance of the requirement part. Entities can still choose to define the term 'like replacements' within their own programs and processes if the Registered Entity deems that necessary or a value add. The word "any" was removed from the Measures for Requirement R3 Part 3.3 as requested. Regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;", the SDT agrees this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. This bullet was removed in response to this industry concern.

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

For requirement 1.1.2, we suggest to simply write, "Verify the required cyber security controls remain implemented". There is confusion as to why "…as required as a part of the change" adds to the requirement.

However, the newest version is closer to what is done by industries. Old version address the case when a plan made its own programs in assembly language. Now, it's more representative of the real world when third-party software executables are buy and install in systems.

{C}1) It is unclear if Management Interface of Cyber System is in scope for CIP-010

{C}2) The usage of ¨OR¨ seems to allow entities not to control changes to software. Suggest using the ¨AND¨ instead in ¨Control the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007¨

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document that their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls.

Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with "Control the implementation of intended changes to software, or intended changes to settings . . ." Part

1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”

For Part 3,3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term. “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s.

For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.”

For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Regarding Part 1.1.2 and the unintended implication that that entities must verify all “required cyber security controls remain implemented as required”, the SDT separated the requirement for verification of security controls from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur 'as a part of the change' authorized in Part 1.1, and scoped Those verification actions to what was relevant to the changes so a complete compliance check for CIP-005 and CIP-007 is not required.

Yes, the Management Interface of a Cyber System is in scope for CIP-010. CIP-005 contains specific requirements for the controls that must be implemented for a Management Interface where the Glossary term is used within the Requirement or Requirement Part in CIP-005. A Management Interface is a component of a Cyber System, so where changes to the Management Interface's implemented cyber security controls serving the requirements in CIP-005 occur, those changes would be subject to CIP-010 requirements.

The SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance.

The SDT agrees the use of "AND" vs "OR" in relation to the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."

Also considered were comments for Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, modifications were made to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed. The intent is to require active vulnerability assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented or when failures occur, and existing Cyber Assets need to be replaced. The risk is associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another Cyber Asset that has been configured like the one being replaced suggests the security posture is known as a function of the reconstruction process to build the replacement, and because the existing Cyber Asset had been previously assessed, thereby not warranting the performance of the requirement part. Entities can still choose to define the term 'like replacements' within their own programs and processes if the Registered Entity deems that necessary or a value add.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
In the proposed language, the term "could weaken" as it applies to changes requiring configuration management controls is vague and, as undefined, leaves the determination unsupported by existing definitions. GSOC suggests either substituting "alters" or adding " . . . as determined by the responsible entity". As proposed, change management controls would only need to be utilized for a type of change that undermines existing security and not for all changes. Additionally, as proposed, the language of 1.1.2 could subject the responsible entity to double jeopardy violationof CIP-010 as well as the underlying violations of CIP-005 and CIP-007.. Additionally, as written, every control must be reviewed for every applicable change regardless of whether it is technical, procedural, or impacted by the change. GSOC recommends the removal of 1.1.2 as a separate requirement and inclusion in measures.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused the Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.".	

Regarding Part 1.1.2 and the unintended implication that that entities must verify all “required cyber security controls remain implemented as required”, the SDT separated the requirement for verification of security controls from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur as a part of the change authorized in Part 1.1, and scoped those verification actions to what was relevant to the changes so a complete compliance check of CIP-005 and CIP-007 is not required.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP appreciates SDT’’s efforts in making requirements more clear. However, AEP does not support R1.2 and R2.1 and states recommendations below. • **R 1.2.1**: SDT added **“the configuration of”** as in “…where the test is performed in a manner that minimizes adverse effects to ensure **that the configuration of** required cyber security controls in CIP-005 and CIP-007 reamin implemented as required”. AEP suggests removing this added language as it is too prescriptive. • **R2.1**: AEP questions the statement "*unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007*" and recommend SDT to revert the requirement languages as proposed in Draft #3, i.e., “Methods to monitor for unauthorized changes at least once every 35 calendar days. Document and investigate detected unauthorized changes.”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees with your comments about the prescriptive nature of the language "the configuration of" in proposed Part 1.2.2 and removed that language. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R2 Part2.1. The SDT removed this language and refocused Requirement R2 Part 2.1 on methods to monitor for "...unauthorized changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement part CIP-007, as defined by the Responsible Entity."	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	

Comment	
Constellation supports comments that were submitted by Exelon Corporation. Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See response to Exelon Corporation.	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation supports comments that were submitted by Exelon Corporation. Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDTs response to Exelon Corporation.	
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 comments written in the EEI response	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDTs response to EEI.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
R1-Removing baseline configuration does not change what needs to be done in practice. Entities will still need to retain a baseline configuration as evidence from which to establish the changes that were authorized. · For Part 1.1 an entity will still need to show the baseline configuration prior to the change to show required cyber security controls in CIP-005 and CIP-007 are not adversely affected. · For Part 2.1 an entity will still need to provide baseline configurations for evidence that they monitor at least once every 35 calendar days for unauthorized changes to the items listed Parts 1.1 and 1.2. For R3-the concern is that Remediation VLANs should be properly defined in the technical rational or Glossary as it may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees entities will need a means to demonstrate changes that alter the behavior of one or more cyber security controls serving one or more requirement parts in CIP-005 or CIP-007 were authorized in accordance with Requirement R1 Part 1.1, and maintaining a baseline is one method an entity can choose to demonstrate their practices. The SDT considered your comments regarding Remediation VLANs and reviewed TR related to this functionality. The SDT did not create a new Glossary of Terms definition.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	

Answer	No
Document Name	
Comment	
In large part, the proposed changes are fine. However, there is an implication by virtue of the new veribiage and removal of “baseline configurations” that additional configuration items (outside of the original “baseline configuration”) need to be included within change management. Such additional configuration items are not explicitly included in the Measures section, thus leaving this aspect of the requirement wholly subjective. Additionally, the third bullet on slide 39 from the Project 2016-02 Webinar seems to implicitly add a documentation requirement for the analysis/comparison of baseline configurations to security controls. This ask is not in the requirement. Including it in the Webinar presentation empowers Regional auditors to ask for evidence of requirements that are not included in the standard or measures sections.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT considered the suggestion to reintroduce the word 'baseline' so R1 would provide clarity on 'how' to meet the requirement using a 'baseline'. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", and which changes then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way how an entity can choose to demonstrate compliance. The SDT reviewed TR based on comments provided to ensure the baseline part is clear and understood. Lastly, the SDT agrees Requirement R1 does NOT include a documentation requirement for the analysis/comparison of baseline configurations to security controls.	
Kristine Martz - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	

AWS agrees with changes to CIP-010 R1, R2, and R3. However, AWS remains concerned that CIP-010 R4 does not address security risks associated with virtual machines (VM) hosted on physical Transient Cyber Assets (TCAs) because the standard language states that a VM running on a physical TCA can be treated as software. We acknowledge the SDT response to the previous comments in the consideration of comments, but we still see security risks and have provided our previous comment below for context.

The Standard allows an entity to choose one or a combination of security controls that may not extend cyber security protections to the VM itself leaving VMs potentially vulnerable to security threats undetected by the physical host. We propose removing the language "Virtual machines hosted on a physical TCA can be treated as software on that physical TCA" from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT considered your concerns and concluded that a VM on a TCA would be considered software on the TCA and subject to Requirement R4, Attachment 1 from that perspective. Additional information can be found in the TR.

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

Answer	No
Document Name	

Comment

The current phrasing of Part 1.1.2 implies that entities must verify all "required cyber security controls remain implemented as required" for any change to software or security settings even if the change itself does not impact a certain control (e.g. a windows patch typically doesn't modify an ESP/EAP for CIP-005, updating a FW Policy does not impact CIP-007 R2, etc.). This new language removes entities abilities to identify potential impacts and verify/test those impacts as allowed by the in-effect standard and the previous revision. Entergy is concerned that this language as written would require entities an undue burden to re-verify non-impacted controls for every change. While the Measures section implies that an entity has latitude to identify which cyber security controls should be verified (" a list of cyber security controls verified") this is not clearly aligned with the language of the standard.

Entergy recommends adding clarifying language to CIP-010 R1 Part 1.1 that entities verify potentially impacted cyber security controls, such as "Verify the required cyber security controls ***identified by the Responsible Entity that could be weakened*** remain implemented as required as part of the

change." This would allow entities to focus verification efforts on potentially impacted controls based on the nature of the change, instead of a one-size fits all approach of re-verifying every CIP-005 and CIP-007 control for every change.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Regarding Part 1.1.2 and the unintended implication that that entities must verify all "required cyber security controls remain implemented as required", the SDT separated the requirement for verification of security controls from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur as a part of the change authorized in Part 1.1 and scoped those verification actions to what was relevant to the changes so a complete compliance check of CIP-005 and CIP-007 is not required. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
In large part, the proposed changes are fine. However, there is an implication by virtue of the new veribiage and removal of "baseline configurations" that additional configuration items (outside of the original "baseline configuration") need to be included within change management. Such additional configuration items are not explicitly included in the Measures section, thus leaving this aspect of the requirement wholly subjective. Additionally, the third bullet on slide 39 from the Project 2016-02 Webinar seems to implicitly add a documentation requirement for the analysis/comparison of baseline configurations to security controls. This ask is not in the requirement. Including it in the Webinar presentation empowers Regional auditors to ask for evidence of requirements that are not included in the standard or measures sections.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", and which changes then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way how an entity can choose to demonstrate compliance. The SDT reviewed TR to ensure the baseline part is clear. Lastly, Requirement R1 does NOT include a documentation requirement for the analysis/comparison of baseline configurations to security controls.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
CIP-010 R2.1 as written would require an audit of every setting that could impact a CIP-005 or CIP-007 security control every 35 calendar days on High Impact devices. For some devices, this could be hundreds of individual settings, and Cyber Assets may not provide these settings in a way that audit of those settings could be automated. This would also effectively be a baseline configuration, though a more rigorous one than required by the currently effective requirements, as each setting would have a “baseline” to ensure the effectiveness of the security control it implements. Chelan finds it difficult to develop a requirement that accomplishes the same security objective CIP-010 R2.1 of auditing that unauthorized changes have not occurred without the development of a baseline configuration to compare against. By definition, auditing changes requires you to have a known good state, essentially a baseline configuration. If the SDT wishes to eliminate baseline configurations, it should eliminate the periodic monitoring for unauthorized changes, or change the security objective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees there is potential for confusion, or perceived scope increase or misinterpretation by use of terms like "settings" would be interpreted as too prescriptive, so this phrasing was removed.	

After careful consideration, the SDT chose not to reintroduce the word 'baseline', and chose to keep the monitoring component in Requirement R2 by providing greater clarity on the scope and objectives of each requirement. The prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can choose to continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007..." require authorization per Requirement R1 Part 1.1. Changes to high impact BES Cyber Systems and their associated 1. EACMS; and 2. PCA, and SCI supporting an Applicable System in Requirement R2 Part 2.1 are then subject to the monitoring requirements in Requirement R2 Part 2.1. The SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear. Additionally, The SDT refocused Requirement R2 Part 2.1 on methods to monitor for "...unauthorized changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement part CIP-007, as defined by the Responsible Entity." to further ensure this requirement is not misinterpreted as a mini audit of CIP-005 and CIP-007.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	

Similar to the MRO-NSRFs response, WEC Energy Group wishes to bring attention to the added phrase in CIP-010 Requirement 1 Part R1.1, “…or intended changes to settings that could weaken configured cyber security controls required by CIP005 and CIP-007.” We also would raise concerns with the current proposed Measures for R1.1.

This language raises questions. On applicable systems, are entities expected to authorize/monitor for both software changes AND settings that could weaken cyber security controls. Or does the ‘or’ indicate that choosing one of those would fulfill the obligations? For instance, consider a password change on a service account/agent which unintentionally breaks logging capabilities on an unspecified BCA. While an entity would be in violation of CIP-007 R4, with this new CIP-010 language, would the password change constitute a “change to settings” which weakened a CIP-007 control (R4.2) and therefore have been required to navigate the change management process? Would simply changing an applicable password from 10 characters to 9 characters constitute a weakening of CIP-005/CIP-007 cyber security controls?

There are many configuration changes that currently don’t affect one of the baseline items but could be considered in scope in the new version of the standard (for example, modification of anti-virus settings or any configuration settings on a firewall). This addition, combined with one of the statements made during the September 12, 2022 webinar that entities may have more compliance work to perform under the revised CIP-010, indicates that the scope of change management is broadened under the proposed revisions. This directly contradicts other statements that have

stressed how the revisions are to be backwards compatible. The idea being that any entity that is in compliance today with current technologies and processes will be compliant under the revised standards, even if they do not seek to employ or utilize virtualization technologies.

We recommend the SDT to revisit the proposed CIP-010 R1.1 language and undertake any further revision needed to ensure that the scope of CIP-010 R1 is not expanded any more than necessary. One recommendation would be to separate both R1.1 into two parts, one addressing BCAs only, which would mirror existing CIP-010-3 R1.1 language, and one addressing SCI specifically which would further clarify “settings” (this would also necessitate splitting the proposed R2.1 into two different requirements as well).

Secondly, it seems that there continues to be confusion in the industry over whether or not to baseline and what are the best methods by which to demonstrate compliance with CIP-010 R1.1. We note that, while the Measures for R1.1 are quite lengthy, all the detail is about what the “documented process” should address or include, without suggesting examples of what the documented process could actually be documented as. We approve of providing options for entities to comply with CIP-010 R1.1 without necessarily having to maintain and demonstrate a documented baseline but it’s also true that many utilities wish to continue using precisely that approach for their compliance – yet the word baseline is missing entirely from the Measures section of CIP-010 R1.1. We understand that “documented process” that includes the various items listed implies a baseline, but there is no reason we see not to just then come out and say “baseline” is an example of an acceptable option.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Also see response to MRO NSRF. The SDT agrees the on terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused the Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."

Regarding the potential for confusion, perceived scope increase or misinterpretation by the use of terms like "settings" would be interpreted as too prescriptive, so this phrasing was removed.

The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", then require authorization per Requirement R1 Part 1.1.

The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.	
Tim Kelley - Tim Kelley 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; - Tim Kelley, Group Name SMUD / BANC	
Answer	No
Document Name	
Comment	
The new proposed wording is challenging to navigate and subjective. For example, what does it mean to weaken the configured cybersecurity controls and settings? We recommend changing CIP-010 R1.1 back to the previous wording, and restore previous requirement parts through R2.1, and add “SCI supporting an Applicable System in this Part”. This change is out of scope to support virtualization other than adding SCI to the applicability column. The proposed changes do nothing to support virtualization but do add significant ambiguity to the requirement. Also, a baseline MUST be established if there is going to be a requirement to monitor for unauthorized changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.". The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007..." then require authorization per Requirement	

R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The MRO NSRF wish to bring attention to the added phrase in CIP-010 Requirement 1 Part R1.1, "…or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007." The MRO NSRF also would raise concerns with the current proposed Measures for R1.1.

This language raises questions. On applicable systems, are entities expected to authorize/monitor for both software changes AND settings that could weaken cyber security controls. or does the 'or' indicate that choosing one of those would fulfill the obligations? For instance, consider a password change on a service account/agent which unintentionally breaks logging capabilities on an unspecified BCA. While an entity would be in violation of CIP-007 R4, with this new CIP-010 language, would the password change constitute a "change to settings" which weakened a CIP-007 control (R4.2) and therefore have been required to navigate the change management process? Would simply changing an applicable password from 10 characters to 9 characters constitute a weakening of CIP-005/CIP-007 cyber security controls?

There are many configuration changes that currently don't affect one of the baseline items but could be considered in scope in the new version of the standard (for example, modification of anti-virus settings or any configuration settings on a firewall). This addition, combined with one of the statements made during the September 12, 2022 webinar that entities may have more compliance work to perform under the revised CIP-010, indicates that the scope of change management is broadened under the proposed revisions. This flies in the face of other statements that have stressed how the revisions are to be backwards compatible and that any entity that is in compliance today with current technologies and processes will be compliant under the revised standards even if they do not seek to employ or utilize virtualization technologies.

Secondly, it seems that there continues to be confusion in the industry over whether or not to baseline and what are the best methods by which to demonstrate compliance with CIP-010 R1.1. The MRO NSRF note that, while the Measures for R1.1 are quite lengthy, all the detail is about what the "documented process" should address or include, without suggesting examples of what the documented process could actually be documented as. The MRO NSRF approve of providing options for entities to comply with CIP-010 R1.1 without necessarily having to maintain and demonstrate a documented baseline but it's also true that many utilities wish to continue using precisely that approach for their compliance – yet the word baseline is missing entirely from the Measures section of CIP-010 R1.1. The MRO NSRF understand that "documented process" that includes the various items listed implies a baseline, but there is no reason the MRO NSRF see not to just then come out and say "baseline" is an example of an acceptable option.

The MRO NSRF recommend that the first paragraph of R1.1 Requirement be rewritten to read, "Control the implementation of intended changes to Applicable Systems that could weaken configured cyber security controls required by CIP-005 and CIP-007." The MRO NSRF also recommend the inclusion of the word "baseline" as an example in the R1.1 Measures of a type of documented process that Registered Entities may employ to

demonstrate their compliance with R1.1. Alternatively, if this recommendation is not acceptable, then some other change in verbiage that provides Entities the option of either continuing to comply using current baseline and baseline deviation tracking methods, or allowing a different approach per the new requirement and measure language, to ensure for the allowance of backward compatibility.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity." Regarding the same terminology for Requirement R2 Part 2.1, the SDT refocused Requirement R2.1 on methods to monitor for "...unauthorized changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement part CIP-007, as defined by the Responsible Entity." The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to confirm an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
In Measures to revised R1.1.2, the only example given of a tool used to verify required security controls [required by CIP-005 and CIP-007] remain implemented is a vulnerability scanner. It is unlikely that this will be the tool used to verify these controls, and that guidance may be misleading to Regional Entity auditors. It is more likely that a configuration management database will be used to verify that software is installed and that controls	

such as listening ports, disabled accounts, password controls, antimalware settings, and applied security patches are unchanged. CEHE recommends that the SDT add “configuration management database” as an example in the Measures in R1.1.2. In R3.3, the exception for replacement of the same type of Cyber System with a configuration of the previous or other existing Cyber System should be revised to include additions of the same type, not only replacements. An example is adding a console from an identical known good image as existing consoles. This is not a replacement, but from a security and reliability perspective, has the same effect. Language should be revised to say “Like replacements or additions of the same type of Cyber System with a configuration of the previous or other existing Cyber System”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT chose to split Requirement R1 Part 1.1.2 back out into Part 1.4 and made modifications to enable virtualization. The measures were rewritten to align with the reinstated Part 1.4. The SDT agrees and made modifications to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
In Measures to revised R1.1.2, the only example given of a tool used to verify required security controls [required by CIP-005 and CIP-007] remain implemented is a vulnerability scanner. It is unlikely that this will be the tool used to verify these controls, and that guidance may be misleading to Regional Entity auditors. It is more likely that a configuration management database will be used to verify that software is installed and that controls such as listening ports, disabled accounts, password controls, antimalware settings, and applied security patches are unchanged. SIGE recommends that the SDT add “configuration management database” as an example in the Measures in R1.1.2. In R3.3, the exception for replacement of the same type of Cyber System with a configuration of the previous or other existing Cyber System should be revised to include additions of the same type, not only replacements. An example is adding a console from an identical known good image as existing consoles. This is not a replacement, but from a security and reliability perspective, has the same effect. Language should be revised to say “Like replacements or additions of the same type of Cyber System with a configuration of the previous or other existing Cyber System”.	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
For R2 Dominion Energy recommends reverting back to the previous language and include verbiage excluding password changes. The term “settings” is too subjective and can be interpreted inconsistently. Additionally, for the Severity Level for R1, Dominion believes the SAR was intended to address virtualization and arbitrarily changing the VSL for R1 is not in scope. Dominion recommends reverting back to the previous language	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the use of terms like “settings” have the potential for confusion, perceived scope increase or misinterpretation would be interpreted as too prescriptive, so this phrasing was removed. The SDT revisited comments regarding VSLs and SAR in preparation for the next draft.	
Israel Perez - Salt River Project - 6	
Answer	No
Document Name	
Comment	
We still have concerns on CIP-010-5 because the draft does not include the Guidelines and Technical Basis section where it defines what must be included in a vulnerability assessment. It is understood that the Standards Drafting team emphasizes backwards compatibility, but, the proposed	

changes to CIP-007 R1 and CIP-010 R1.1 could affect what is required in the vulnerability assessments. At the very least, we would like to know and comment on what additional items will be required for SCI in a vulnerability assessment as there is nothing found in the current proposed changes. Lastly, under CIP-010 R3.3 BES Cyber System is shortened to BCS. However, this is different than the other parts of CIP-010 R3. We recommend consistency.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The reinstatement of Guidelines and Technical Basis (GTB) is out of scope for the project 2016-02 SAR. The Technical Rationale Transition Plan to revise the Reliability Standards template to eliminate the GTB section and allow for the creation of a separate document containing the TR was endorsed by the NERC Standards Committee on January 17, 2018. The use of the term "guideline" in GTB has created confusion for some stakeholders on the use of information in this section for guidance in developing compliance approaches, and the TR for Reliability Standards team was formed to clarify the intended use of information in this section, and to address that confusion. The purpose of this project was to further clarify the principles, development, and use of GTB (historically) and TR. The ERO continues to assess compliance based on the language of the Reliability Standard and the facts and circumstances presented. With the enactment of the Compliance Guidance Policy, it appears helpful to further clarify the distinction between Implementation Guidance and GTB (or TR, as explained below). GTB should focus on TR that assists technical understanding of a requirement and/or Reliability Standard. GTB should not include compliance examples or compliance language. Such information, if needed, should be developed as Implementation Guidance under the Compliance Guidance Policy. As a result, the SDT established a separate TR document. Any Implementation Guidance proposed by the SDT must go through the ERO endorsement process. Additionally, the SDT took another pass through the draft to assure consistency with the use of the acronym BCS for BES Cyber System throughout.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes modifications to CIP-010 should be limited to conforming changes only.	
Likes 0	
Dislikes 0	

Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern disagrees with Part 1.1 Requirements that includes the phrase “settings that could weaken cyber security controls required by CIP-005 and CIP-007”. Southern finds this phrase overly broad, questioning if full compliance could ever be proven out of the universe of “settings” (registry settings, configuration paramenters, per application settings, etc.). Added to the complexity of knowing all settings is the phrase “could weaken” adding in the idea of ‘potential’ to this already elusive scope. Southern suggests the SDT reconsider the concept used in draft 3 of the entity defining the higher level types of changes they have in their change management programs. In addition, to provide further clarity of scope, Southern suggests the SDT go through CIP-005 and CIP-007 and list the areas that should be under CIP-010 change management. Since these requirements are the same for every entity, that list should be the same for every entity.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The language “…changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007” is subjective. There could be any number of “settings” that “could weaken” the security controls. Can guidance be given such as some exapmples of these settings that could be	

used to weaken the security controls? Also, is “software patches” synonymous with “security patches” or are these two (2) different entities of their own?	
Likes 0	
Dislikes 0	
Response	
The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity." Additionally, modifications were made to remove concerns of unintended nuances from using synonymous terms interchangeably. Cyber security patches is now the term used throughout.	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
We feel using “could” in parts of CIP-010-5 is very subjective and is not necessary. Further the measures uses “may” instead of “could”. A change either does or doesn’t affect cybersecurity controls required by CIP-005 and CIP-007. We are fine with the language, but feel it would be cleaner and less ambiguous without “could”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the requirement language must be clear and unambiguous as to ‘what’ is required and removed the word "could". The SDT chose to keep the word "may" within the Measures because the data in this column is intended to provide examples of possible ways an entity can demonstrate compliance, but it is not the only way nor is it a requirement. The flexibility of 'how' through the use of "may" in the Measures is appropriate.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes

Document Name	
Comment	
EEI supports the revisions made to CIP-010 for Draft 4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
NEE requests the SDT apply linkages in CIP-010-5 R1 P1.1 to all subparts for software scope. Suggest clarity that all subparts refer back to the software scope definition established in CIP-010-5 R1 P1.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT modified the Parts that hinge on the scoping in Part 1.1. by adding "change from Part 1.1" to provide clear linkage and scoping.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments that were submitted by the MRO NERC Standards Review Forum.	

Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the modification made to CIP-010, but PG&E provides the following recommendation: The text of "…intended changes to settings ..." withing the Requirement language be clarified to avoid un-intended consequence of setting changes that would not have an impact on the CIP-005 and CIP-007 controls from being brought into scope of Audit Teams.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the potential for confusion, perceived scope increase or misinterpretation by use of terms like "settings" would be interpreted as too prescriptive, so this phrasing was removed.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy supports the revisions for CIP-010-5, but harbors some concern regarding unclear language in Requirement R1, subpart 1.1. The word "settings" does not enjoy the same clarifying language as does the word "software". We believe this creates a risk for unpredicatble interpretation without any additional technical rationale defining the intent of the word. NV Energy suggests "settings" receive a definition complementary to "software" to better assist entities reach compliance, but ultimately feels the language in its current state is workable although not ideal.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the potential for confusion, perceived scope increase or misinterpretation by use of terms like "settings" would be interpreted as too prescriptive, so this phrasing was removed.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes to CIP-010 but feel the following "weaken" statement introduced in part R1.1, without an official definition, leads to uncertainty and lack of clarity around the items that may fall into change management. This will result in re-examination of existing systems and baselining methodologies that threaten the intended backwards compatibility of the new requirements. In addition, we agree with EEI stance that which “settings” are in scope requires additional clarification.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity." Also see response to EEI regarding comments on the term "settings".	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

BPA believes CIP-010 R2.1 needs a verb in front of beginning of the Requirement language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See parent Requirement R2 for the verb, as the action is "to implement".	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
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 Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
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	
Donna Wood - Tri-State G and T Association, 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	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	

Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE continues to be concerned security obligations will be reduced by removing an explicit requirement for Registered Entities to create and maintain baseline configuration documentation.

Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 5), CM-2 Baseline Configuration, which states, “Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.”

NIST Special Publication 800-53 (Rev. 5) provides additional information, such as using tools to track version numbers on operating systems, applications, types of software installed, and current patch levels in order to maintain the currency, completeness, accuracy, and availability of the baseline configurations of systems. This is information that is currently captured within existing baseline documentation requirements.

If the drafting team has concerns that maintaining baseline documentation of dynamic VMs is not technically feasible, Texas RE suggests adding the verbiage “per system capability” to CIP-010 R1’s baseline requirements. Registered Entities have demonstrated that the vast majority of systems, both physical and virtual, are capable of having baseline documentation created, tracked, and updated as necessary. As such, this requirement should remain in place for those systems where it is technically feasible to perform this industry best security practice.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to confirm an entity can continue using baselines as the method to determine which changes "...alter the

behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed TR to ensure the baseline part is clear.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying CIP-010 to allow for more flexibility in tracking changes to applicable systems while maintaining and even increasing security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	

7. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes or scoping clarifications related to SCI. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
As mentioned earlier, disagree with adding R1.6 to CIP-005 as CIP-005 is written for protections of logical devices and data. This should be restored back to CIP-006 R1 Part 1.10.f7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT feels that R1.6 consolidates requirements together and removes the possibility for double jeopardy.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST disagrees with proposed changes to CIP-003 and CIP-011 due to the fact proposed changes go beyond conforming changes. NST disagrees with proposed changes to CIP-009, as omitting SCI from all Requirements and Parts except for R1 Part 1.5 it would establish "implied requirements," as discussed in our comments on Question 9, below. NST acknowledges that in some recovery situations, it might only be necessary to recover a virtual BES Cyber System and not its supporting SCI. However, given that failure or destruction of an SCI could, in some scenarios, wipe out an entire Control Center, NST believes that inclusion of SCI in a Responsible Entity's recovery plan(s) should be mandatory rather than a suggested best practice.	

NST agrees with proposed conforming changes to CIP-004, CIP-006, CIP-008 and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP-009's focus is to ensure that the BCS can be recovered. An Entity can choose to recover that functionality of the BVCS in any manner that restores that functionality, potentially without the use of SCI, even if the original BCS included the use of SCI. Additionally, the majority of organizations making use of virtualization today will choose the All-In model where the underlay is classed as a part of the BCS itself. In this instance the underlay (not technically SCI) would be subject to the recovery requirements.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT disagrees as many will not vote to approve terms (particularly technology terms) and definitions in a vacuum with no context as to how those definitions will be used. At times terms are created to match the requirements, such as IRA. Many may say that the IRA definition is too restrictive. However it is defined so that it matches scenarios where the CIP-005 R2 requirements can be met without affecting functionality or reliability of systems.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	

Comment
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;" Request clarification on execution of what? Perhaps "execution" should be changed to "entity use" For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC For CIP-006, Part 1.3 consider changing from "per system capability" because "per system capability" is an inadvertent get-out-of-jail. For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2 For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with "all" in the new language. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the vendor . . ." The R1 applicable systems language is "for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI)." We suggest that the scope should be "applicable systems," not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change. CIP-003 Attachment 1 references to the bullet that started with "Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill. The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC.

The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable. The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves. The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;" Request clarification on execution of what? Perhaps "execution" should be changed to "entity use" For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC For CIP-006, Part 1.3 consider changing from "per system capability" because "per system capability" is an inadvertent get-out-of-jail. For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2 For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with "all" in the new language. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the vendor . . ." The R1 applicable systems language is "for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI)." We suggest that the scope should be "applicable systems," not all software and patches by the vendor.	

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change.

CIP-003 Attachment 1 references to the bullet that started with “Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill.

The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC.

The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable.

The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves.

The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.

Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC

Answer	No
Document Name	

Comment

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident

For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;” Request clarification on execution of what? Perhaps “execution” should be changed to “entity use”

For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC For CIP-006, Part 1.3 consider changing from “per system capability” because “per system capability” is an inadvertent get-out-of-jail. For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2 For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with “all” in the new language. The new Part 1.2.5 says “ Verification of software integrity and authenticity of all software and patches provided by the vendor . . .” The R1 applicable systems language is “for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI).” We suggest that the scope should be “applicable systems,” not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change.

CIP-003 Attachment 1 references to the bullet that started with “Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill.

The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC.

The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable.

The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves.

The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	No
Document Name	
Comment	
Same comment as for CIP-010, Q6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response to Q6.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident For CIP-003, Attachment 1, 5.1, requests clarification of the new bullet which says "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;" Request clarification on the execution of what? Perhaps "execution" should be changed to "entity use" For CIP-004, R5 requests confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC For CIP-006, Part 1.3 consider changing from "per system capability" because "per system capability" is an inadvertent get-out-of-jail. For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2 For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with "all" in the new language. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the	

vendor . . .” The R1 applicable systems language is “for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI).” We suggest that the scope should be “applicable systems,” not all software and patches by the vendor.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change. CIP-003 Attachment 1 references to the bullet that started with “Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill. The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC. The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable, as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable. The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves. The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	

For CIP-003, Attachment 1, Section 4, request confirmation that, while this Section has no updates, this Section's scope is being expanded because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident .

For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;" The language should be clarified to explain the word "execution" (i.e., on execution of what?) Perhaps "execution" should be changed to "entity use".

For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents due to the updated definitions of IRA and ERC.

For CIP-006, Part 1.3 consider changing from "per system capability" because "per system capability" is an inadvertent "get-out-of-jail free card.

For CIP-011, the double jeopardy between R2 and Part 1.2 should be clarified.

For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. The use of the word "all" in the new language is of concern. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the vendor . . ." The R1 applicable systems language is "for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI)." The scope should be "applicable systems," not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change.

CIP-003 Attachment 1 references to the bullet that started with "Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill.

The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC.

The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity

to prove that the system is not capable, as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable. The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves. The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No: Application Containers need to be defined with additional clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for additional clarification on the reasoning behind treatment of application containers as software of a VCA or CA.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	No
Document Name	
Comment	
For CIP-006, Part 1.3, consider changing from "per system capability" to "if technically feasible" because "per system capability" is an inadvertent get-out-of-jail. *For CIP-011, the SRC requests clarification on the double jeopardy between R2 and Part 1.2. Both sections apply to the handling and use of BCSI. If you violate R2, you will have mishandled or misused R1.2.*	

For CIP-013, Part 1.2.5, consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with "all" in the new language. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the vendor . . ." The R1 applicable systems language is "for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI)." We suggest that the scope should be "applicable systems," not ***"all"*** *software and patches by the vendor.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable, as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable. The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves. The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.	
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 conforming changes or scoping clarifications related to SCI made to the various CIP standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed conforming changes to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying the rest of the CIP Standards to allow for implementing future technologies while maintaining and even increasing security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E supports the conforming changes to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
For the proposed CIP-008, the Applicability would include, “An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or Shared Cyber Infrastructure supporting a BES Cyber System.” Note that by a literal reading of this, an SCI supporting EACMS would not be in scope for CIP-008 whereas a traditional EACMS would be.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This appears to be a redlining issue. The working copy for Draft 5 showed the correct SCI applicability Statement.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
For the proposed CIP-008, the Applicability would include, “An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or Shared Cyber Infrastructure supporting a BES Cyber System.” Note that by a literal reading of this, an SCI supporting EACMS would not be in scope for CIP-008 whereas a traditional EACMS would be.	

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your comment. This appears to be a redlining issue. The working copy for Draft 5 showed the correct SCI applicability Statement.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments that were submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
See response to MRO.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	

Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the conforming changes and scoping clarifications made to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
(1) The proposed language in in CIP-006-7, R1, Part 1.3, points to system capability, but there are concerns with situations where the PACS is capable, but there is a limitation with a particular physical access device. It seems as thought that may present a gap in the proposed language. As an example, an entity currently has a TFE for a limited physical access device where two factor cannot be applied, such as a roof hatch where it is not possible to install a locking mechanism controlled by the PACS system. Under the approved TFE, additional measures are taken to secure that physical access point. The concern with the proposed language is that the roof hatch may be seen as a physical access device rather than a system. In this instance, the PACS is capable of two-factor authentication, but two-factor authentication cannot be applied to that particular physical access device. Because of this potential and unintended gap, we recommend using the language "per system or device capability." **(2) For CIP 009-7, Requirement R1, Part 1.1, please consider adding the language SCI supporting an Applicable System" in the Applicable Systems column**.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. CIP-006 R1.3 has been discussed extensively, and the SDT position is that the per system capability does apply at the system level, and the system is capable in the instance you present. However, there are components of the system that may not be, and the intent is to enforce the additional authentication method wherever components of the system support this capability.	

CIP-009's focus is to ensure that the BCS can be recovered. An Entity can choose to recover that functionality of the BCS in any manner that restores that functionality, potentially without the use of SCI, even if the original BCS included the use of SCI. Additionally, the majority of organizations making use of virtualization today will choose the All-In model where the underlay is classed as a part of the BCS itself. In this instance the underlay (not technically SCI) would be subject to the recovery requirements.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
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	
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	

Israel Perez - Salt River Project - 6	
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	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley 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; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
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	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 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	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	

8. The SDT has revised the Implementation Plan to include 3 defined early adoption dates as options should Responsible Entities choose to do so. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
PNMR believes early adoption of the revised CIP standards and definitions is beneficial but proposes that Responsible Entities are not tied to only three early adoption choices (6, 12, or 18 months) after approval of the new standards. PNMR proposes that Responsible Entities still follow notifying their Regional Entities of their early adoption choice within fifteen calendar days of making that decision, but that Responsible Entities have the ability to early adopt at any time between 6 months and 24 months. If, for example, a Responsible Entity is not able to early adopt at the 6-month mark but would be able to 8 months after the approval of the new standards, the Responsible Entity should be able to early adopt and not have to wait an additional 4 months until the 12-month mark. An alternate proposal would be for the Responsible Entity to notify the Regional Entity of its 6, 12, or 18-month early adoption date but have the ability to change its early adoption date if it is realized before the agreed-upon early adoption date that the Responsible Entity would not be able to be compliant with the new standards by that date. In this case, the Responsible Entity could move its early adoption from 6 months to 12 months, for example.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The implementation plan allows for 3 specific early adoption dates that will be set to ensure that all entities are being held to the same date to reduce any confusion that may occur during any audits that may cross those periods. The SDT will add a clarifying note in the implementation plan.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment	
With the implementation of compliance oversight plans (COP)s, many entities, particularlylarger entities, are experiencing more frequent audits. 36 months may be more appropriate for an implmentation period based on the scope of the changes being proposed under this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT asserts that the existing 24 month time period is sufficient while considering the level of the backward compatible language that exists for most requirements. No changes were made to this longstanding portion of the language. It will carry forward from previously and currently approved versions of the implementation plan.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

EEI supports the revised Implementation Plan as proposed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
RF agrees with the inclusion of the 3 defined early adoption dates as options should Responsible Entities choose to do so with the understanding that all Standards and Requirements will be adopted at that same time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the revised Implementation Plan and the three (3) defined early adoption dates.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Xcel Energy supports EEI comments and thanks the SDT for working on creating an implementation plan that will allow for enough time for a successful implementation while also allowing for early implementation for entities looking to employ virtualized technologies at a faster pace.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern understands and agrees with the revised implementation plan which includes 3 defined early adoption dates as an option. Southern also understands that if one of the options were chosen, we would have 15 calendar days to notify our Regional Entity of the selected option.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
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	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
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	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
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	

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
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	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley 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; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	

Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
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	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 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	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
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	
Donna Wood - Tri-State G and T Association, 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	
Glen Farmer - Avista - Avista Corporation - 5	
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	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	

Dislikes 0	
Response	
See response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE continues to be concerned there is conflicting language in the planned changes section of the implementation plan, as well as language in the unplanned changes section in the proposed implementation plan that could result in a reliability gap.

Regarding the conflicting language addressing planned changes, Texas RE notes that the second paragraph in the proposed implementation plan states: “For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.”

Texas RE understands this language to mean the BCS at the substation must be compliant upon the commissioning of the substation. Texas RE agrees with this position.

However, the first and third paragraphs in the proposed implementation plan appears to conflict with this reading. Specifically, the first paragraph states: “Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.” Furthermore, the proposed implementation plan’s third paragraph states: “For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.”

Texas RE understands this language to mean the BCS at the substation is not required to be compliant until the Registered Entity has performed its annual assessment under CIP-002 R2. This introduces a reliability gap as assets that were commissioned shortly after the entity has completed a CIP-002 R2 evaluation will not be required to be evaluated for up to 15 calendar months, and therefore would not be required to be compliant with the applicable cyber security requirements. Texas RE does not agree with this position. Additionally, there are no requirements to identify PACS, EACMS, or PCAs.

Regarding the proposed implementation plan's concerning unplanned changes, Texas RE is concerned the language could be read to result in a reliability gap. Specifically, the first paragraph of the implementation plan states "Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2." Texas RE notes that while it is true that during a CIP-002 R2 review an entity may discover that a BCS now meets a higher BCS threshold than it previously held, this is not the only situation in which an entity may become aware of the need for a higher categorization. For example, if an entity is informed by their RC, PC, or TP that an asset is critical to the derivation of an IROL then the knowledge that the systems must meet the medium impact criteria is immediate and as such the 12-month timer to implement medium impact controls should begin immediately. As written, the language in the implementation plan could result in a situation where a Registered Entity could delay the implementation of medium impact controls at such a substation or power plant for up to 27 calendar months, if the IROL notification arrived immediately after a CIP-002 R2 evaluation. Texas RE recommends the SDT revise the proposed implementation plan language around "unplanned changes" to preclude this result.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. No changes have been made to this longstanding portion of the language. It will carry forward from previously and currently approved versions of the implementation plan. These changes are considered out of scope for the current 2016-02 project as it relates to Virtualization, IRA, or the remaining V5TAG items.	

9. Please provide any additional comments for the standard drafting team to consider, if desired.
Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	
Document Name	
Comment	
N/A	
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	
Southern suggests that the definition for “Cyber System” be modified to eliminate the “A group of” language and simply begin with “One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDTs modified the Cyber System definition.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	
Document Name	
Comment	

NST disagrees with the SDT decision to not compel Responsible Entities to identify and maintain a list of SCI that support BES Cyber Systems in CIP-002. In order to demonstrate compliance with various CIP-003 – CIP-013 requirements for SCI, a Responsible Entity would surely have to demonstrate that all its SCI were accounted for. NST is aware of the fact there is no existing CIP requirement to maintain an inventory of “associated” devices including PCAs, EACMS, and PACS, but doing so was some years ago memorably characterized by a well-known representative of a Regional Entity as an "implied requirement." NST believes an SDT goal should be to avoid adding to the list of "implied requirements."

NST believes the proposed “Exemption” statement in every CIP Standard, 4.2.3.3, “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an Electronic Security Perimeter (ESP) that extends to one or more geographic locations” is both confusing and inaccurate. One provides for the confidentiality and integrity of data, not ESPs. N&ST suggests rewording that’s consistent with the language of proposed CIP-005 Requirement R1 Part 1.4, such as “Cyber Systems associated with communication links used to span a single ESP among two or more geographic locations.”

NST notes the second of two proposed "Measures" for CIP-007 R1 Part 1.3 suggests evidence of compliance with the "non-sharing" of SCI CPU and memory requirement could include "Hardware partitioning of physical Cyber Assets." If our understanding of "hardware partitioning" is correct (that it means, for example, all the Medium Impact BCS that co-reside with High Impact BCS on a single hardware platform are moved to different hardware), then according to the proposed definition of SCI, the end result of "hardware partitioning" would be one or more hardware platforms that are no longer SCI, which would render all proposed requirements for SCI, including CIP-007 R1 Part 1.3, inoperable.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Project 2021-03 Group B will look into the inclusion of the identification and maintenance of a list of SCI (and EACMS, PACS, and PCAs) that support BES Cyber Systems.

Exemption 4.2.3.3 intends to exclude the devices that may not be owned/operated by the Registered Entity, but carry the data between relevant locations which are all treated as a single ESP. This is necessary because the entity may have no ability to perform the required controls for these assets that would otherwise be considered in the same ESP as an applicable BCS. The control objective of the associated CIP-005 R1 Requirement is to ensure that this exclusion does not compromise the integrity or confidentiality of the data that traverses this link.

The Measures of CIP-007 R1 Part 1.3 second bullet inclusion of "Hardware Partitioning of physical Cyber Assets" may result in an entity creating an architecture that does not meet the new definition of SCI. It was included to cover the capabilities that systems like LPARs bring to the virtualization discussion, which offer advanced hardware partitioning capabilities initially implemented in the mainframe environment.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	
Document Name	
Comment	
AZPS has no additional comments for the standard drafting team to consider currently.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	
Document Name	

Comment
We still have concerns on CIP-010-5 because the draft does not include the Guidelines and Technical Basis section where it defines what must be included in a vulnerability assessment. It is understood that the Standards Drafting team emphasizes backwards compatibility, but, the proposed changes to CIP-007 R1 and CIP-010 R1.1 could affect what is required in the vulnerability assessments. At the very least, we would like to know and comment on what additional items will be required for SCI in a vulnerability assessment as there is nothing found in the current proposed changes. Lastly, under CIP-010 R3.3 BES Cyber System is shortened to BCS. However, this is different than the other parts of CIP-010 R3. We recommend consistency.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The SDT investigated the option of re-introducing the guidance from the previous GTB section of CIP-010-3. This guidance section is in a CIP-010-4 Implementation Guidance document that was been submitted to the ERO for endorsement by the Project 2019-03 Drafting Team: https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-010-4_Implementation_Guidance_Redline_07282020.pdf The SDT also addressed the inconsistency of acronym use within the Applicable Systems column within the Standard.

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	

Comment
Although not directly revised in this draft, two issues in CIP-007 deserve mention. Requirement 3.3 obstructs smooth updates of antimalware signatures with large administrative cost and compliance risk, for very little, if any, reliability benefit, and is actually impossible with many automated systems today. The requirement should be revised to remove the testing of signatures. Additionally, CIP-007 R5 language inherited from earlier versions requiring at least 8 character passwords is outdated. SIGE suggests requiring at least 15 character passwords, where capable.

Likes 0	

Dislikes 0	
Response	
Thank you for your comments. The issues raised are outside the scope of the Project 2016-02 SAR.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	

Document Name	
Comment	
Although not directly revised in this draft, two issues in CIP-007 deserve mention. Requirement 3.3 obstructs smooth updates of antimalware signatures with large administrative cost and compliance risk, for very little, if any, reliability benefit, and is actually impossible with many automated systems today. The requirement should be revised to remove the testing of signatures. Additionally, CIP-007 R5 language inherited from earlier versions requiring at least 8 character passwords is outdated. CEHE suggests requiring at least 15 character passwords, where capable.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The issues raised are outside the scope of the Project 2016-02 SAR.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports EEI comments and would like to acknowledge the SDT for their hard work over the years in developing a very difficult and technological set of standards that allow for both backward compatibility and inclusion of future technologies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	

N/A	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	
Comment	
PG&E wishes to thank the SDT for their several years of effort in getting these modifications close to completion.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The proposed revised definition for EACMS would add the phrase, “Shared Cyber Infrastructure (SCI)” to the definition. The term “SCI” can refer to a system that is supporting PACS or EACMS. If the definition is read in terms of this type of SCI as it pertains to the EACMS definition, that opens the possibility that the scope of an EACMS could be read as applicable to Cyber Assets that perform electronic access control or monitoring of SCI “EACMS/PACS,” thus potentially creating a hall of mirrors effect. The MRO NSRF are not certain how probable or not such an interpretation may be,	

but prefer that this be addressed here rather than when it's too late to do so. The MRO NSRF ask that the SDT consider this issue and make any edits necessary to address.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your comment. The SDT appreciates the clarity you brought to the concern around the inclusion of SCI as a target of the controls found in the EACMS definition as it was in Draft 4 and modified the EACMS definition.	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	
Document Name	
Comment	
See comments provided by Mike Magruder and/or Glenn Farmer	
Likes 0	
Dislikes 0	
Response	
See response to Mike Magruder and/or Glenn Farmer.	
Tim Kelley - Tim Kelley 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; - Tim Kelley, Group Name SMUD / BANC	
Answer	
Document Name	
Comment	
The use of the terms routable protocol communications, bi-directional routable protocol connection and IP Protocol communications, throughout the standards and the definitions is inconsistent and should be evaluated to determine the necessity of using this different language. If providing the	

consistency through the standards is not an option, it would be better to put these into the definitions so that entities can differentiate one from the other. The language in CIP-010 R1.1 appears to be getting further away from acceptable language with each iteration of the requirement. Moving requirements to the Measures column does not make the changes any more security objective focused. Same comments for CIP-005 R1.2 in that the requirements to document a reason for routable protocol communications should be in the Requirements and not the Measures. Examples of the justification/reason are fine in the Measures, but the requirements should be in the Requirements column.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT was intentional in each use of the communications phrases, as each has a distinct implementation and impact based on the language used. There are some modifications to language in the applicable Requirements that may provide more clarity to the intended use. Additionally, the definition of IRA has been updated to include “bi-directional” in the latest draft as a result of this input. The SDT included this after determining that the concept was no longer included by way of the reliance on the External Routable Connectivity definition and is an integral part of Interactivity. CIP-010 was the main focus of the Draft 5 changes, and working through the appropriate scoping of the change management processes was a key part of this. The SDT asserts that with the recent changes, the scoping is now at a valuable level to include those items that it should, and avoid those items appropriately. This language was drafted using input from many entities through outreach efforts and discussions with Trade Groups. Thank you for your input on CIP-005 R1 Part 1.2. The SDT modified the Requirement language to clarify the need to include the reason for granting access.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	
Document Name	
Comment	
WEC Energy Group is in agreement with the MRO NSRFs comment - "We also wish to raise attention to the proposed change of using the phrase “per system capability,” in place of the previous phrasing “where technically feasible.” While we do not wish for TFE to remain part of the compliance	

paradigm any longer than necessary, we seek assurance that the phrase “per system capability” will indeed be used as an avenue for Registered Entities to demonstrate compliance instead of an opportunity for auditors to find fault with acceptable security and reliability practices."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See response to MRO NSRF. The concept of "per system capability" is not new. See CIP-007-6 R4 Part 4.1 references to "per BES Cyber System" and "per Cyber Asset capability". The use remains the same, and the burden is on the Entity to document that the system is not capable of performing the required function, the same way the use is mentioned above from CIP-007-6 R4 Part 4.1.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	
Document Name	
Comment	
Chelan asks the SDT to consider the real risks and the goals of the CIP standards. CIP has always been about the protection of BES Cyber Assets/Systems and reducing the risk of a compromise or failure of a BES Cyber System which would adversely impact the BES. By definition, BES Cyber Systems are systems that will have direct impact on the BES, so it makes sense to protect those devices most stringently. Protected Cyber Assets also represent a significant risk since there is no network separation between PCAs and their associated BES Cyber System. A VM escape attack executed against a BES Cyber System would be a single exploit to potentially adversely impact the BES. However, EACMS and PACS devices do not have a direct impact on the reliability of the BES, and are segregated from BES Cyber Systems and Protected Cyber Assets by protections required by CIP-005. A successful VM escape against a EACMS or PACS device would require a second attack for there to be an adverse impact to the BES. The new affinity requirements increase both the risk of an adverse impact, by reducing the availability of the in-scope VMs and increase the risk of non-compliance, by forcing the use of a control not meant for this purpose. The requirements proposed essentially create six groups of devices that potentially may not share CPU or memory: 1) High Impact BCS/PCA (including EACMS and PACS classified as PCAs, excluding Intermediate Systems)	

2) High Impact EACMS/PACS (outside the ESP)

3) Medium Impact BCS/PCA (including EACMS and PACS classified as PCAs, excluding Intermediate Systems)

4) Medium Impact EACMS/PACS (outside the ESP)

5) Potentially Low Impact BCS

6) Out-of-Scope Devices

This means that a RE would have to establish up to 6 separate resource pools to comply with the definition of PCA and the text of CIP-007 R1.3. Assuming you can group devices in the affinity rule sets you create (this may not be possible on all platforms), this would require 15 separate anti-affinity rules, in addition any existing rules required for resource management purposes.

With the updated language suggested in Question 4, there would only be 3 resource pools needed:

1) High Impact BCS/PCAs (including EACMS and PACS classified as PCAs, excluding Intermediate Systems

2) Medium Impact BCS/PCA (including EACMS and PACS classified as PCAs, excluding Intermediate Systems)

3) All other devices.

Only 3 anti-affinity rules are needed here to satisfy the suggested requirements. This greatly reduces the complexity of the DRS rules needed to satisfy the security objective to protect the BES from the threat of VM escape attacks and decreases the risk of that a BES Cyber System is unable to find a host to run in the event of a failure of one or more SCI hosts.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT made changes to the affinity requirements with the intent to create two pools of resources that should not cross where mixed trust exists without high watermarking. Specifically, resources associated with High or Medium Impact BCS or their associated EACMS, PACS or PCA, would be in one pool and Low Impact BCS and non-CIP systems would be in another resource pool. This should simplify the implementation, while maintaining the security benefit that isolating our most critical systems from those less trusted.

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

Answer	
Document Name	
Comment	
MPC supports comments that were submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	
Kristine Martz - Amazon Web Services - 7	
Answer	
Document Name	
Comment	
The SDT is clear that this project SAR focuses on on-premise virtualization, however, many virtualization concepts convey use of cloud. AWS suggests explicitly stating whether these new terms/requirements, specifically SCI, will apply to cloud or not. If these terms/requirements do not apply to cloud, it should be obvious to the reader.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SAR does not include an overall look at CIP standards for situations where Cyber Systems are owned/operated by non-registered entities. The SDT is simply defining what SCI is. There is a possibility the definition will apply to infrastructure not owned/operated by the registered entity, when the Standards are modified to provide for this capability in the future.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	

Document Name	
Comment	
Conflating support for both High-, Medium-, and Low-Impact Cyber Assets within a single Virtualization Cluster will create additional questions and interpretations between Responsible Entities and ERO Enterprise staff. Clusters by their very nature include pools of shared SCI to include CPU, Memory, Disk, and network resources that are shared between all Cluster members to allow for balancing resources, recovery from failed hardware, and maintaining high availability. The complexity required to balance these pooled resources using affinity rules or logical boundaries to disallow different impact levels of VM guests from running on the same physical resources could be high. Moving VM guests can take place without the need for clustering and would allow for segregated siloing of different impact Cyber Assets without the requirement of determining high-water marking every time a VM guest is moved. Communications play a key role in determining the current health and configuration of clusters – especially with heartbeats and SCSI data requests. Responsible Entities have a high bar to assure that these communications are not to the point that they create common networking connections that would start to include additional VM Guests as PCA. Marrying both ESP and zero-trust within an overall ESP would better serve our Responsible Entities and create a more secure environment as zero-trust Cyber Assets would not be internet-facing while simplifying the management of the environment. Maintaining the ESP, and fully incorporating virtualization and zero trust paradigms within an identified ESP allows Responsible Entities to leverage another layer of defense (defense-in-depth) for BCS by limiting ingress/egress points and access to these Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT made changes to the affinity requirements with the intent to create two pools of resources that should not cross where mixed trust exists without high watermarking. Specifically, resources associated with High or Medium Impact BCS or their associated EACMS, PACS or PCA, would be in one pool and Low Impact BCS and non-CIP systems would be in another resource pool. This should simplify the implementation, while maintaining the security benefit that isolating our most critical systems from those less trusted. The current definition and requirement language in Draft 5 is meant to allow both the old boundary based ESP and modern zero-trust architectures, without precluding one or the other. Requiring a boundary based ESP is counter to zero-trust, since it is applied as close to the affected processes as possible, and everywhere there is an enforcement point in between.	
Todd Bennett – Associated Electric Cooperative, Inc. – 3, Group Name AECI	
Answer	

Document Name	
Comment	
"Responsible Entity" is used multiple times in the CIP standards and is not a defined term or a proposed defined term. The standard drafting team may consider defining this term in the NERC Glossary of Defined Terms. AECI supports the efforts and commitment of the standards drafting team to 296industry when soliciting feedback and proposing solutions to identified gaps in the draft standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Responsible Entity is defined in Section 4.1 at the top of the Standards.	
Alison Mackellar - Constellation - 5	
Answer	
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends clear and concise language on the categorization and impact rating the hosting virtualization infrastructure should have. Specifically, Texas RE recommends eliminating the Shared Cyber Infrastructure definition. Virtualization infrastructure should inherit the highest impact rating and categorizations of the VCAs that the virtualization infrastructure is hosting. For example, if virtualization infrastructure is hosting two high impact BCS, three PCAs associated with high impact BCS, and an EACMS associated with high impact BCS, then the virtualization	

infrastructure should be categorized as a high impact BCS. Implementing high watermarking practices would ensure that the virtualization infrastructure is more reliable and secure. Texas RE continues to note that no matter how many controls are applied there will always be a parent and child relationship between host and VM's. If the hypervisor is compromised, then all VM's can be. Additionally, if a VM is compromised the same can be true, other VM's and the Hypervisor can be impacted. The Hypervisor should be high watermarked to whatever VMs are on it. Any VMs on the hypervisor should also be marked at the highest impact rating. Different applicable systems with varying impact level lends itself to mixed-trust concepts. This change potential opens the door to allow more corporate based systems (payroll, custom software, etc.) to be on the same hypervisor as CIP applicable systems. CPU and memory segregation only may not protect from vulnerabilities such as hyperjacking, VM escape, Denial of Service, etc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Applicable Systems insertion of "SCI supporting an Applicable System in this Part" enforces a High Watermark for the SCI itself. This SCI statement is cascaded throughout the CIP Standards with only a few exceptions, where the requirement language does not support the inclusion. If there are significant deviations in treatment which do not support this, the SDT would like to be made aware of them.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	

Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
See Response to EEI.	
Jodirah Green - ACES Power Marketing - 6	
Answer	
Document Name	
Comment	
We would like to thank the Project 2016-02 SDT on their hard work, dedication, and continuing to listen to industry feedback to meet the FERC order and not create significantly more compliance burden.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Diana Torres - Imperial Irrigation District - 6	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	
Document Name	
Comment	
It is unclear in the draft CIP-002-7 how the classification hierarchy is impacted. What is the hierarchy of the SCI classification? Is dual classification with SCI expected??	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See the CIP-002 TR and Definitions Rationale for how the hierarchy is applied to SCI. In essence this is applied through the inclusion of "SCI supporting an Applicable System in this Part".	

Wesley Maurer - Wesley Maurer On Behalf of: Teresa Krabe, Lower Colorado River Authority, 5, 1; - Wesley Maurer	
Answer	
Document Name	
Comment	
LCRA would like to seek clarification regarding virtualization of EACMS outside of an ESP. If the host has in-scope EACMS as well as out of scope virtualized machines, would the same rules apply as SCI within a the ESP? There would be SCI associated with an EACMS. There would be an EACMS that is a virtual machine. Are affinity rules the only compliance obligation associated with the out of scope VM?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Referring to the Applicable System column within the CIP Standards where the phrase "SCI supporting an Applicable System in this Part" exists and an SCI supports an EACMS associated with either the HIBCS, or some form of MIBCS, the requirements apply to both the EACMS and SCI that support it. This applies to the Affinity requirement as well as Applicable Systems, not the out of scope VM. However, applying an affinity rule to Applicable VMs would enforce an anti-affinity rule for out of scope VMs by practice.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
LCRA would like to seek clarification regarding virtualization of EACMS outside of an ESP. If the host has in-scope EACMS as well as out of scope virtualized machines, would the same rules apply as SCI within a the ESP? There would be SCI associated with an EACMS. There would be an EACMS that is a virtual machine. Are affinity rules the only compliance obligation associated with the out of scope VM?	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Referring to the Applicable System column within the CIP Standards where the phrase "SCI supporting an Applicable System in this Part" exists and an SCI supports an EACMS associated with either the HIBCS, or some form of MIBCS, the requirements apply to both the EACMS and SCI that support it. This applies to the Affinity requirement as well as Applicable Systems, not the out of scope VM. However, applying an affinity rule to Applicable VMs would enforce an anti-affinity rule for out of scope VMs by practice.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	
Document Name	
Comment	
In future postings, for definitions, it would be helpful if the table for the definitions could include each standard where the definition appears. *In closing, SRC reiterates that our gravest concern is with proposed changes to CIP-010, Part 1.1 and Part 2.1 which do away with the concept of "baseline changes." The proposed language of "settings changes" goes beyond what was previously in the CIP standards such that we believe they are no longer backwards compatible. SRC proposes "settings changes" be modified to "configuration changes" or eliminated altogether.* *Additionally, the SRC would like for the SDT to consider that the standards process has taken very long and there are newer technologies that are not being addressed with these changes.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Definitions Table has been modified to include references to where the definition is used. The language of CIP-010 R1 was the main focus of the Draft 5 changes. See the revised language which makes use of the "configuration changes" concept.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	

Alliant Energy supports the comments submitted by the MRO NSRF	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	

End of Report